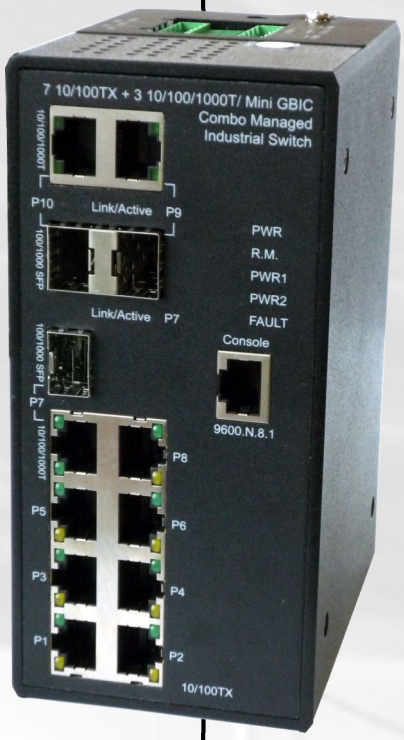
N967

Managed industrial switch



User manual

EQUITEL

About this manual …

This document is the technical reference of the model **N967**, an 7 10/100TX + 3 10/100/1000T/SFP modules combo - Managed Industrial Switch -

.

© Equipos De Telecomunicación Optoelectrónicos, S.A.
Zaragoza, Spain, Sep. 2011
Ed. 1.0

Equipos de Telecomunicación Optoelectrónicos, S.A.
Polígono de Malpica, c/ F oeste, G. Quejido, nave 74
50057 Zaragoza SPAIN
Tel. +34 976 570 353
Fax +34 976 571 383
E-mail: mail@equitel.es
www.equitel.es

The information included in this manual cannot be copied or reproduced in any way without the previous written authorisation of Equipos de Telecomunicación Optoelectrónicos, S.A.

Content

Introduction 1
Features 1
Software Specification 3
Package Contents 5
Hardware Description 6
Physical Dimension 6
Front Panel 6
Top View 7
LED Indicators 8
Ports 10
Cabling 13
Wiring the Power Inputs 17
Wiring the Fault Alarm Contact 18
Mounting Installation 19
DIN-Rail Mounting 19
Longear Mount Plate Mounting 21
Hardware Installation 22
Installation Steps 22
Network Application 23
Pro-Ring II Application 24
Daisy-Couple Ring 24
Multi-Couple Ring 25

Advanced Dual Homing 25
Console Management 26
Connecting to the Console Port 26
Pin Assignment 27
Login in the Console Interface 27
CLI Management 29
Commands Level 29
Commands Set List 31
System Commands Set 31
Port Commands Set 34
Trunk Commands Set 37
VLAN Commands Set 38
Spanning Tree Commands Set 40
QOS Commands Set 43
IGMP/MLD Commands Set 44
Mac / Filter Table Commands Set 45
SNMP Commands Set 46
Port Mirroring Commands Set 48
802.1x Commands Set 49
TFTP Commands Set 52
SystemLog, SMTP and Event Commands Set 52
SNTP Commands Set 54
Pro-ring II Commands Set 56
Web-Based Management 57
About Web-based Management 57
Preparing for Web Management 57

System Login 58
System Information 59
IP Configuration 60
DHCP Server – System configuration..... 61
DHCP Server – Client Entries..... 62
DHCP Server - Port and IP Bindings 63
TFTP - Update Firmware 64
TFTP – Restore Configuration 64
TFTP - Backup Configuration 65
System Event Log – Syslog Configuration..... 65
System Event Log - SMTP Configuration 67
System Event Log - Event Configuration 69
Fault Relay Alarm 71
SNTP Configuration 71
IP Security..... 75
User Authentication..... 76
Digital Input/Output 78
Port Statistics 80
Port Control..... 81
Port Trunk 83
Aggregator setting 83
Aggregator Information 85
State Activity..... 86
Port Mirroring 87

Rate Limiting 88
VLAN configuration 89
VLAN configuration - Port-based VLAN 90
802.1Q VLAN..... 93
Rapid Spanning Tree 97
RSTP - System Configuration 97
RSTP - Port Configuration 99
SNMP Configuration 101
System Configuration..... 101
Trap Configuration 102
SNMPV3 Configuration..... 103
QoS Configuration 107
QoS Policy and Priority Type 107
Port-based Priority 109
COS Configuration..... 109
TOS Configuration 109
IGMP Configuration 110
Pro-Ring II System..... 111
Security 114
802.1X/Radius Configuration 114
MAC Address Table..... 117
Factory Default..... 120
Save Configuration 121
System Reboot 121
Troubles shooting 122
Technical Specification..... 122

Introduction

The 7 10/100TX + 3 10/100/1000T with 100/1000M SFP Combo Industrial Managed Switch with DIDO is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. Using fiber port can extend the connection distance that increases the network elasticity and performance.

Features

- System Interface/Performance
  - RJ-45 ports support Auto MDI/MDI-X Function
  - SFP (mini-GBIC) supports 100/1000 Dual Mode
  - Store-and-Forward Switching Architecture
  - Back-plane (Switching Fabric): 7.4Gbps
  - 1Mbits Packet Buffer
  - 8K MAC Address Table
- Case/Installation
  - IP-30 Protection
  - DIN-Rail and Wall Mount Design
- Power Supply
  - Wide-range Redundant Power Design
  - Power Polarity Reverse Protect
  - Overload Current Protection
- Spanning Tree
  - Supports IEEE 802.1d Spanning Tree
  - Supports IEEE 802.1w Rapid Spanning Tree
- VLAN
  - Port Based VLAN
  - Supports 802.1 Q Tag VLAN
  - GVRP
- Pro-Ring II

- X-ring II, Advanced Dual Homing, Daisy Couple Ring and Multi-Coupling Ring Topology
- Provides redundant backup feature and the recovery time below 10ms

- Port Trunk with LACP
- Supports IEEE802.1ab LLDP
- QoS (Quality of Service)
  - Supports IEEE 802.1p Class of Service
  - Per port provides 4 priority queues
  - Port Base, Tag Base and Type of Service Priority
- Bandwidth Control
  - Supports Rate-based and Priority-based Ingress Rate Limiting
  - Broadcast/Multicast Packet Filter Control
- Port Mirror: Monitor traffic in switched networks
  - TX Packet only
  - RX Packet only
  - Both of TX and RX Packet
- System Event Log
  - System Log Server/Client
  - SMTP e-mail Alert
  - Relay Alarm Output System Events
- Security
  - Port Security : MAC address entries/filter
  - IP Security: IP address security management to prevent unauthorized intruder
  - Login Security: IEEE802.1X/RADIUS
- SNMP Trap
  - Device cold start
  - Power status
  - Port Link up/Link down
- IGMP with Query mode for Multi Media Application
- TFTP Firmware Update, System Configuration Restore and Backup

- Provides EFT protection 3,000 V_{DC} for power line
- Supports 6,000 V_{DC} Ethernet ESD protection
- Supports DIDO function

Software Specification

Management	SNMP v1, v2c and v3 management Web interface management Telnet interface management Command Line Interface (CLI) management
SNMP MIB	RFC 1215 Trap RFC 1213 MIBII RFC 1157 SNMP MIB RFC 1493 Bridge MIB RFC 2674 VLAN MIB RFC 1643 RFC 1757 RSTP MIB Private MIB
VLAN	Port based VLAN IEEE802.1Q Tag VLAN (256 entries)/VLAN ID (up to 4k in number which can be assigned from 1 to 4096) GVRP (256 groups)
Port Trunk with LACP	LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members
LLDP**	Supports LLDP that allows the switch to advertise its identity and capabilities on the LAN
Spanning tree	IEEE802.1d spanning tree IEEE802.1w rapid spanning tree.

Pro-Ring	Supports X-ring II. Provides redundant backup feature and the recovery time below 10ms
Quality of service	The quality of service determined by port, Tag and IPv4 Type of Service, IPv4/IPv6 Different Service
Class of service	Supports IEEE 802.1p class of service, per port provides 4 priority queues
Port Security	Supports 100 entries of MAC address for static MAC and another 100 for MAC filter
Port mirror	TX packet only RX packet only, Both of TX and RX packets
IGMP	Supports IGMP snooping v1, v2 and v3 Up to 256 multicast groups and IGMP query
IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder
Login Security	Supports IEEE802.1X Authentication/RADIUS
Bandwidth control	Supports ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 100K ~ 250Mbps Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packets The packet filter rate can be set from 100k to 250Mbps
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Supports System log record and remote system log

	server
SMTP	Supports SMTP Server and 6 e-mail accounts for receiving event alert
Relay Alarm	Provides one relay output for port breakdown & power fail Alarm Relay current carry ability: 1A @ DC24V
SNMP Trap	Up to 3 Trap stations Cold start, Port link up, Port link down, Authentication Failure, Private Trap for power status, Power Alarm configuration, Fault Alarm, X-Ring topology change
DHCP	Provides DHCP Client/DHCP Server and IP Relay
DNS	Provides DNS client feature Supports Primary and Secondary DNS Server
SNTP	Supports SNTP to synchronize system clock in Internet
Firmware update, configuration upload/download	TFTP firmware update, system configuration backup and restore Supports binary configuration file for system quick installation

* Future release

** Optional

Package Contents

Please refer to the package content list below to verify them against the checklist.

- 7 10/100TX + 3 10/100/1000T with 100/1000M SFP Combo Industrial Managed Switch with DIDO x 1
- Pluggable Terminal Block x 1

- User manual x 1
- Mounting plate x 2
- RJ-45 to DB9-Female cable x 1

Compare the contents of the industrial switch with the standard checklist above. If any item is damaged or missing, please contact the local dealer for service.

Hardware Description

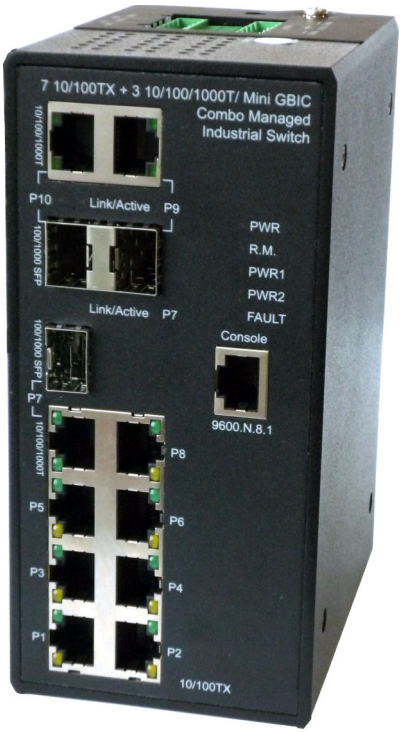
In this paragraph, we will describe the Industrial switch's hardware spec, port, cabling information, and wiring installation.

Physical Dimension

7 10/100TX + 3 10/100/1000T with 100/1000M SFP Combo Industrial Managed Switch with DIDO dimension (W x D x H) is **72mm x 105mm x 152mm**

Front Panel

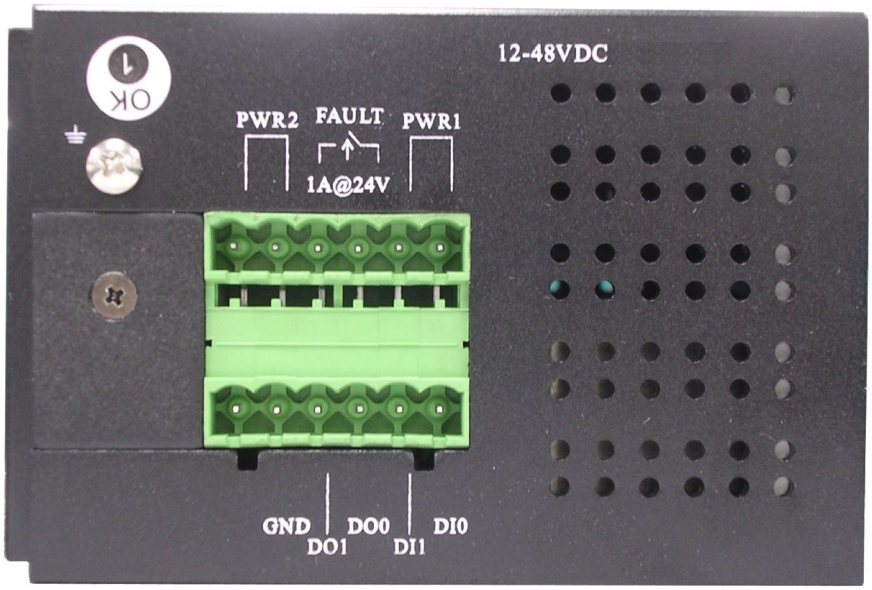
The front panel of the 7 10/100TX + 3 10/100/1000T with 100/1000M SFP Combo Industrial Managed Switch with DIDO is shown as below:



Front Panel of the industrial switch

Top View

The N967 top panel of the 7 10/100TX + 3 10/100/1000T with 100/1000M SFP Combo Industrial Managed Switch with DIDO has one terminal block connector of two DC power inputs.



Top Panel of the industrial switch

LED Indicators

The diagnostic LEDs located on the front panel of the industrial switch provide real-time information of system and optional status. The following table provides description of the LED status and their meanings for the switch.

LED	Status	Meaning
PWR	Green	System power on
	Off	No power inputs
R.M.	Green	The industrial switch is the master device of the X-Ring II group
	Off	The industrial switch is not the master device of the X-Ring II group
PWR1	Green	DC Power 1/AC Power is active

	Off	DC Power 1/AC Power is inactive
PWR2	Green	Power 2 is active
	Off	Power 2 is inactive
Fault	Red	PWR1/PWR2 is inactive
	Off	PWR1 & PWR2 are both active or no power inputs
P1 ~ P6 & P8	Green (Upper LED)	Connected to network
	Blinking (Upper LED)	Networking is active
	Off (Upper LED)	Not connected to network
	Yellow (Lower LED)	Ethernet port full duplex
	Blinking (Lower LED)	Collision of packets occurs
	Off (Lower LED)	Ethernet port half duplex or not connected to network
P7, P9, P10 (10/100/1000T)	Green (Upper LED)	Connected to network
	Blinking (Upper LED)	Networking is active
	Off (Upper LED)	Not connected to network

	Green (Lower LED)	The port is operating at speed of 1000M
	Off (Lower LED)	The port is disconnected or operates at speed of 10/100M
P7, P9, P10 Link/Active (100/1000 SFP)	Green	SFP port is connected to network
	Blinking	Networking is active
	Off	Not connected to network

Ports

- **RJ-45 ports**

The UTP/STP ports will auto-sense for 10Base-T/100Base-TX connections (Fast Ethernet) or 10Base-T, 100Base-TX, or 1000Base-T connections (Gigabit Ethernet). Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling. See the figures below for straight through and crossover cable schematic.

- **RJ-45 Pin Assignments**

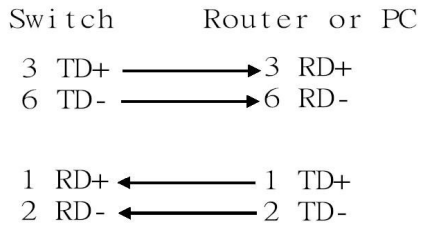
Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

Note *"+" and "-" signs represent the polarity of the wires that make up each wire*

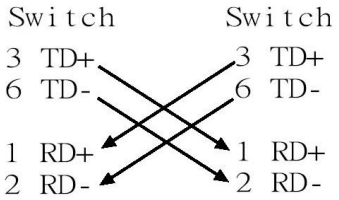
pair.

All ports on this industrial switch support automatic MDI/MDI-X operation, user can use straight-through cables (See figure below) for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The following table shows the MDI and MDI-X port pin outs.

Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)



Straight Through Cable Schematic



Cross Over Cable Schematic

- **3 Gigabit Copper/SFP (Mini-GBIC) combo port:**

The Industrial switch has three auto-detected Giga port—UTP/STP/Fiber combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable for the connection up to 1000Mbps. The small form-factor pluggable (SFP) is a

compact optical transceiver used in optical communications for both telecommunication and data communications. The SFP slots supporting dual mode can switch the connection speed between 100 and 1000Mbps. They are for connecting to the network segment with single or multi-mode fiber. You can choose the appropriate SFP module to plug into the slots. Then use proper multi-mode or single-mode fiber according to the used SFP module. With fiber optic, it transmits at speed up to 1000 Mbps and you can prevent noise interference from the system; the transmission distance depending on the mini-GBIC module is up to 110 km.

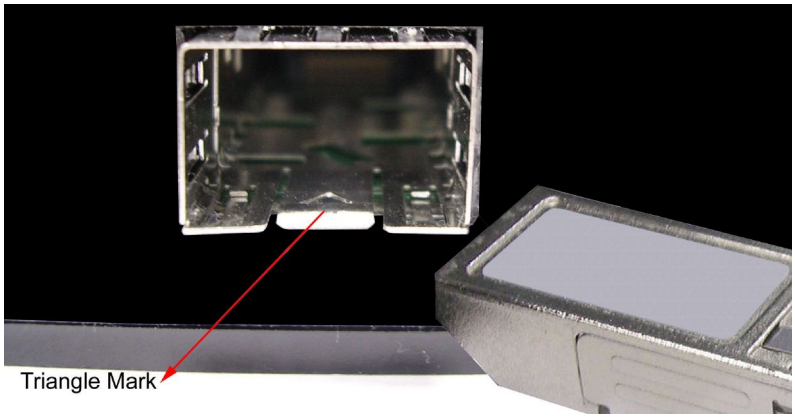
Note	*The SFP/Copper Combo port can't be used at the same time. The SFP port has the higher priority than copper port; if you insert the 1000M SFP transceiver (which is connected to the remote device) into the SFP port, the connection of the accompanying copper port will link down.* *If you insert the 100M SFP transceiver into the SFP port even without a fiber connection to the remote, the connection of the accompanying copper port will link down immediately.* *The user must use the class I optical transceivers which conform to U.S. code of federal regulation, 21 CFR 1040.*

Cabling

Twisted-pair segment can be established by using unshielded twisted pair (UTP) or shielded twisted pair (STP) cabling. The cable between the link partner (switch, hub, workstation, etc.) and the converter must be less than 100 meters (328 ft.) long and comply with the IEEE 802.3ab 1000Base-T standard for Category 5e or above.
Fiber segment using single-mode connector type must use 9/125μm single-mode fiber cable. You can connect two devices in the distance of 10 km. Fiber segment using multi-mode connector type must use 50/125 or 62.5/125μm multi-mode fiber cable. You can connect two devices up to 550m distances.
The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communication applications.

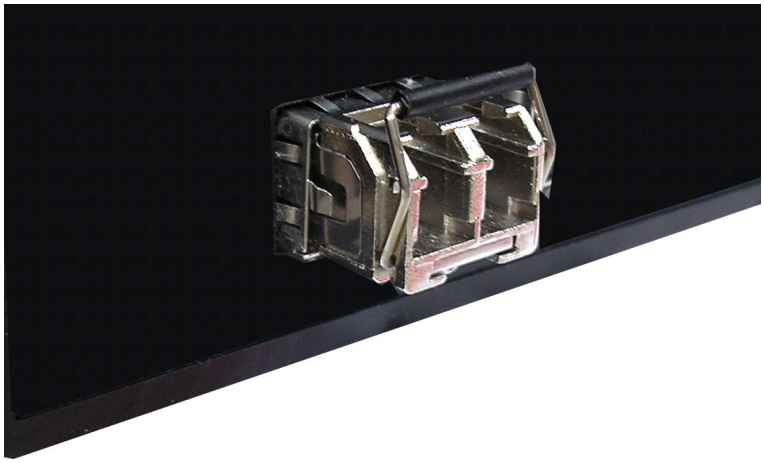
To connect the transceiver and LC cable, please follow the steps shown below:

First, insert the transceiver into the SFP module. Notice that the triangle mark is the bottom of the module.



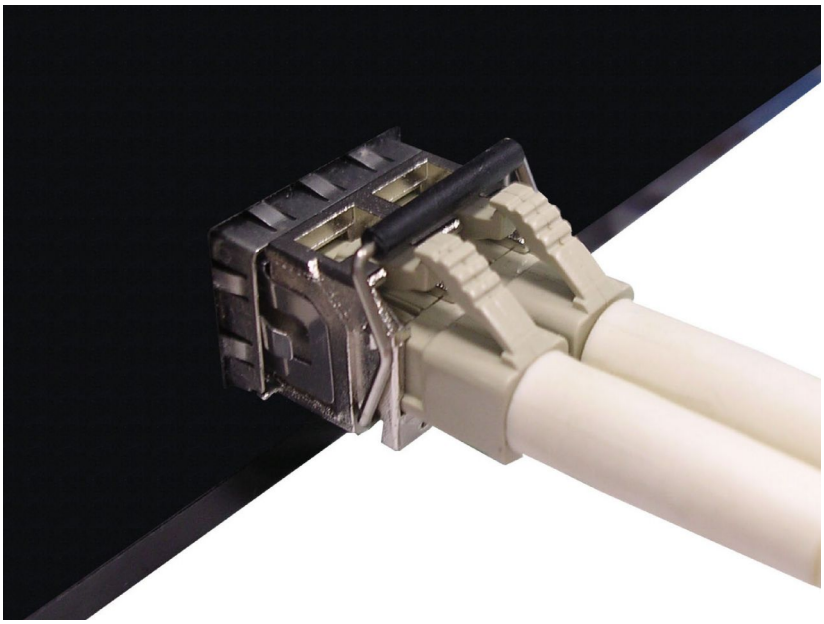
Transceiver to the SFP module

Make sure the module is aligned correctly and then slide the module into the SFP slot until a click is heard.



Transceiver Inserted

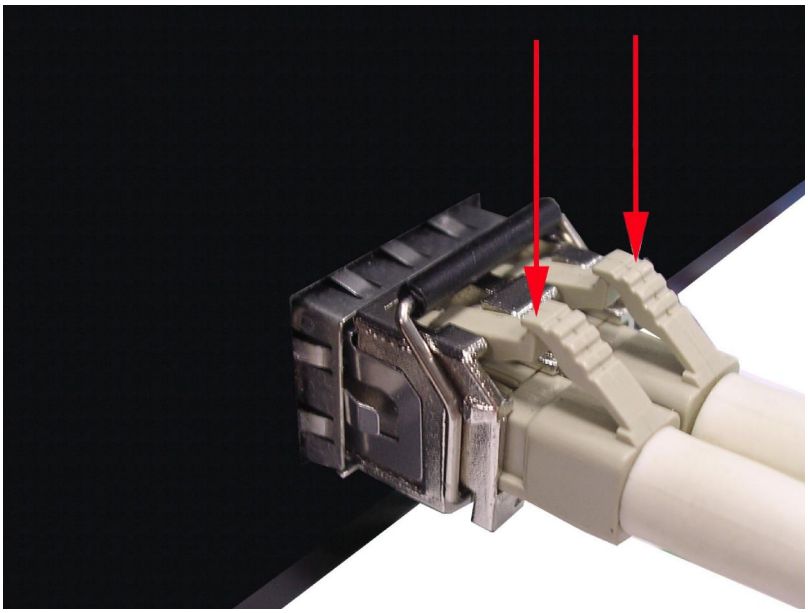
Second, insert the fiber cable of LC connector into the transceiver.



LC connector to the transceiver

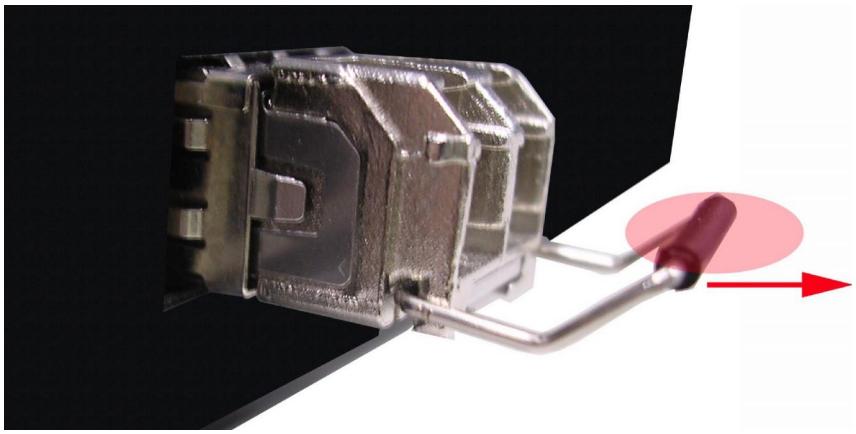
To remove the LC connector from the transceiver, please follow the steps shown below:

First, press the upper side of the LC connector from the transceiver and pull it out to release.



Remove LC connector

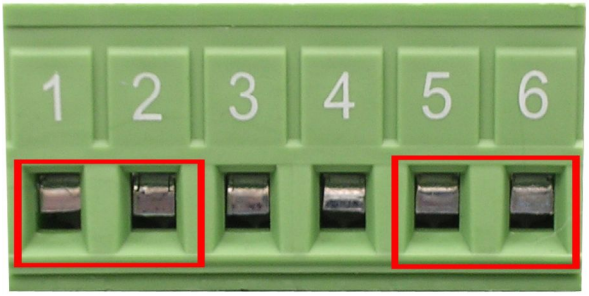
Second, push down the metal loop and pull the transceiver out by the plastic part.



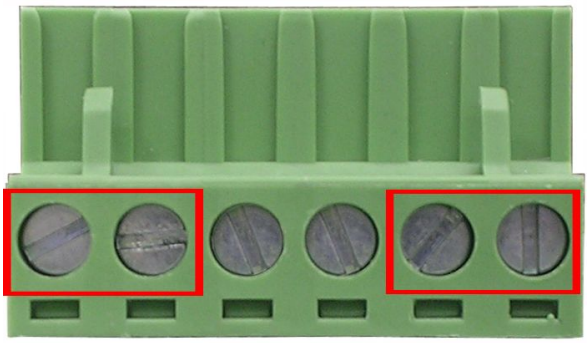
Pull out from the SFP module

Wiring the Power Inputs

Please follow the steps below to insert the power wire.



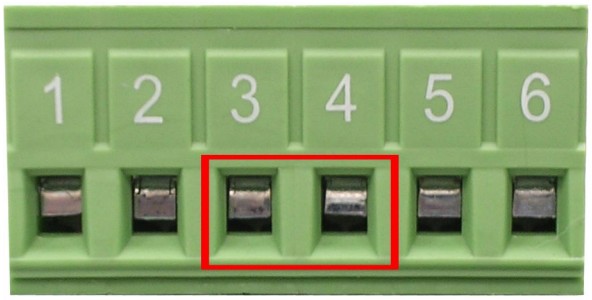
1. Insert AC or DC power wires into the contacts 1 and 2 for power 1, or 5 and 6 for power 2.



2. To tighten the wire-clamp screws for preventing the wires from loosing.

Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of terminal block connector as the picture shows below. Inserting the wires, it will detect the fault status of power failure, or port link failure (for managed model) and form an open circuit.



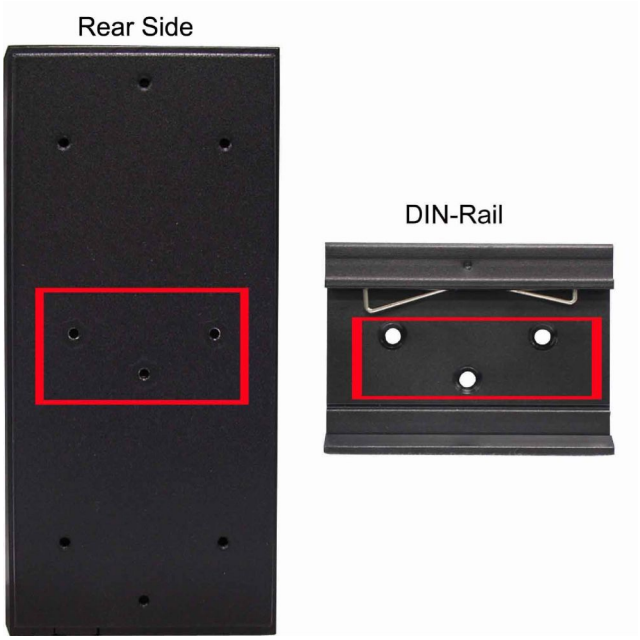
Insert the wires into the fault alarm contacts (No. 3 & 4)

Note	*The wire gauge for the terminal block should be in the range between 12~ 24 AWG.*

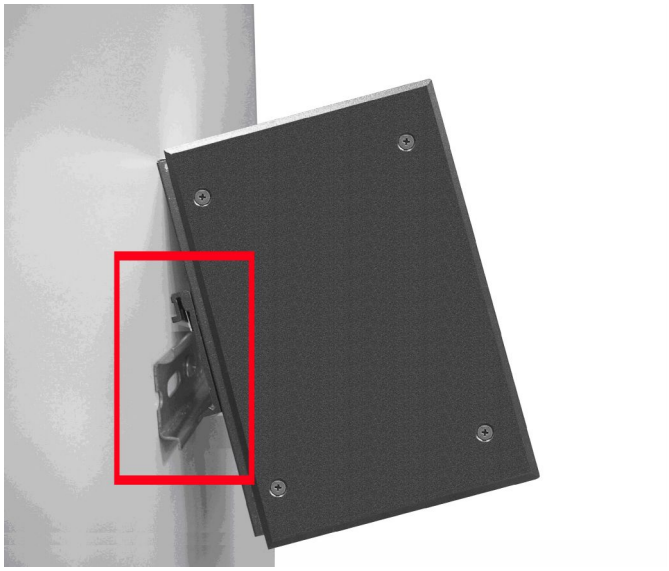
Mounting Installation

DIN-Rail Mounting

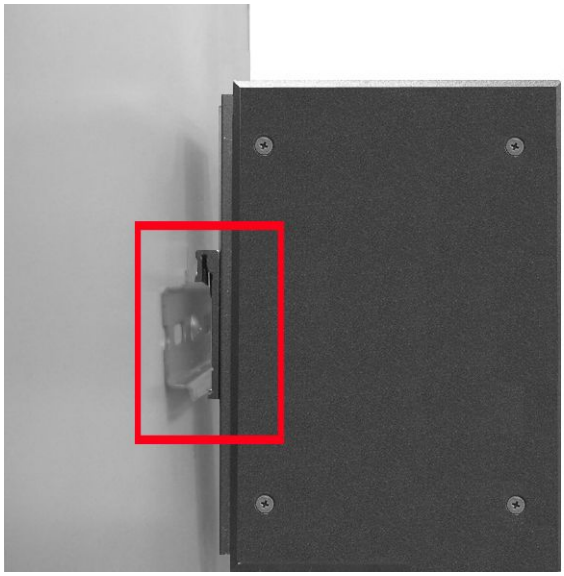
The DIN-Rail is screwed on the industrial switch when out of factory. If the DIN-Rail is not screwed on the industrial switch, please see the following pictures to screw the DIN-Rail on the switch. Follow the steps below to hang the industrial switch.



1. First, insert the top of DIN-Rail into the track.



2. Then, lightly push the DIN-Rail into the track.

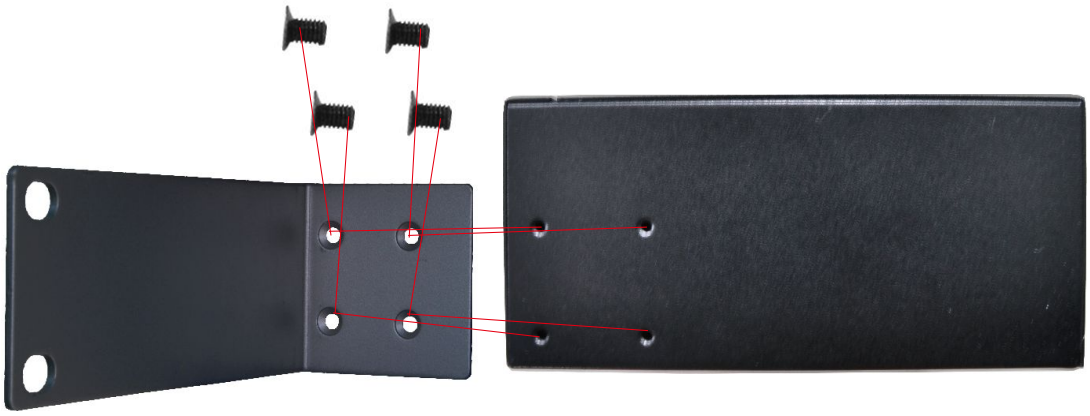


3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the industrial switch from the track, reverse above steps.

Longear Mount Plate Mounting

Follow the steps below to mount the industrial switch with Longear Mount Plate.

1. Place the longear mount plate on the side panel of the industrial switch.
2. Use the screws to screw the Longear Mount Plate on the industrial switch.
3. Use the hook holes at the corners of the longear mount plate to hang the industrial switch on the wall or rack.
4. To remove the longear mount plate, reverse the above steps.



Hardware Installation

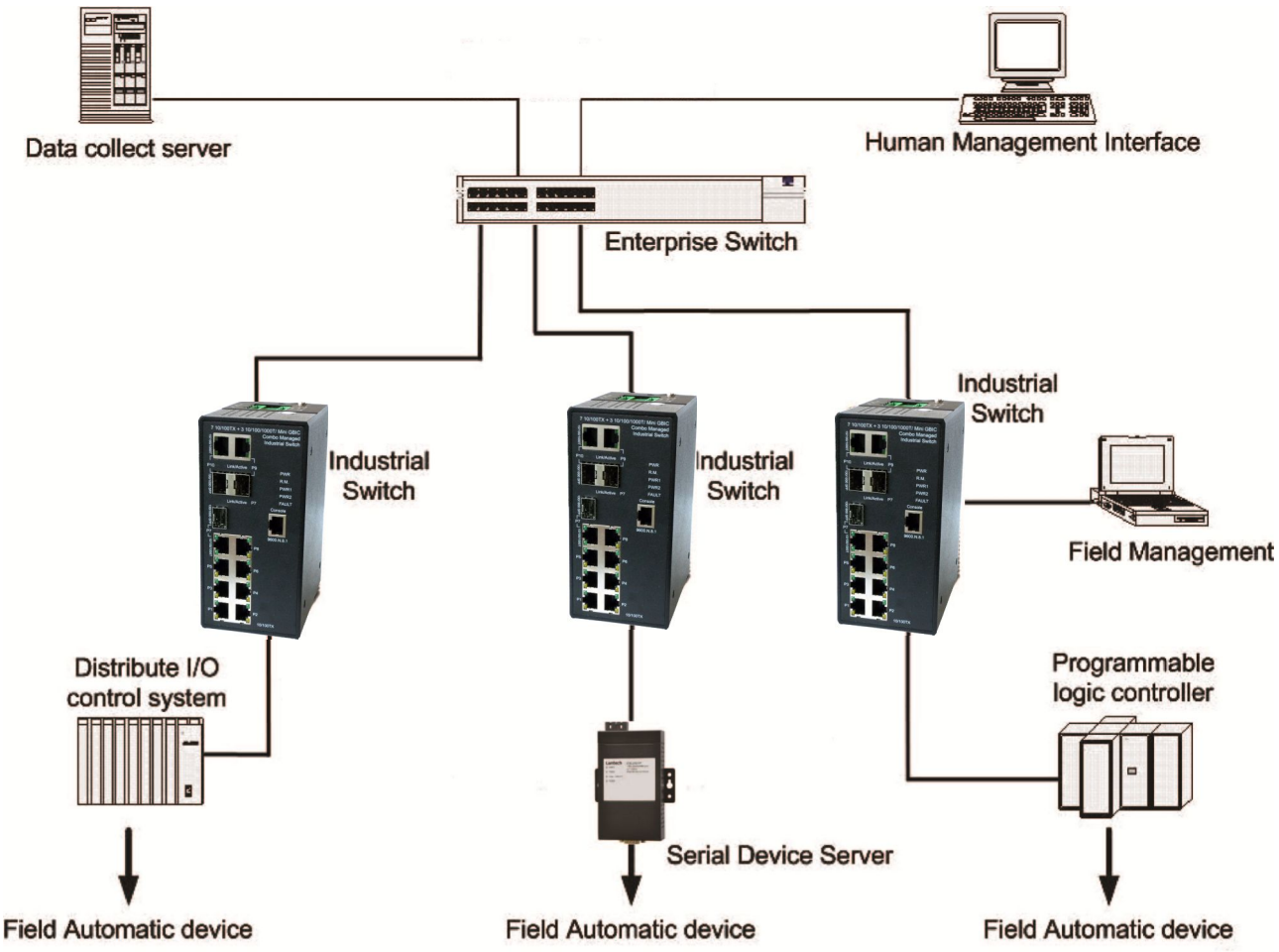
In this paragraph, we will describe how to install the 7 10/100TX + 3 10/100/1000T with 100/1000M SFP Combo Industrial Managed Switch with DIDO and the installation points to be attended to it.

Installation Steps

1. Unpack the Industrial switch packing.
2. Check if the DIN-Rail is screwed on the Industrial switch or not. If the DIN-Rail is not screwed on the Industrial switch, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If the user wants to wall mount the Industrial switch, then please refer to **Longear Mount Plate Mounting** section for Longear Mount Plate installation.
3. To hang the Industrial switch on the DIN-Rail track or wall, please refer to the **Mounting Installation** section.
4. Power on the Industrial switch. Please refer to the **Wiring the Power Inputs** section for knowing the information about how to wire the power. The power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for indication of LED lights.
5. Prepare the twisted-pair, straight through Category 5/above cable for Ethernet connection.
6. Insert one end of UTP/STP cable into the Industrial switch RJ-45 port and the other end to the network device's RJ-45 port, e.g. Switch PC or Server. The RJ-45 port LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.
7. When all connections are set and LED lights all show in normal, the installation is complete.

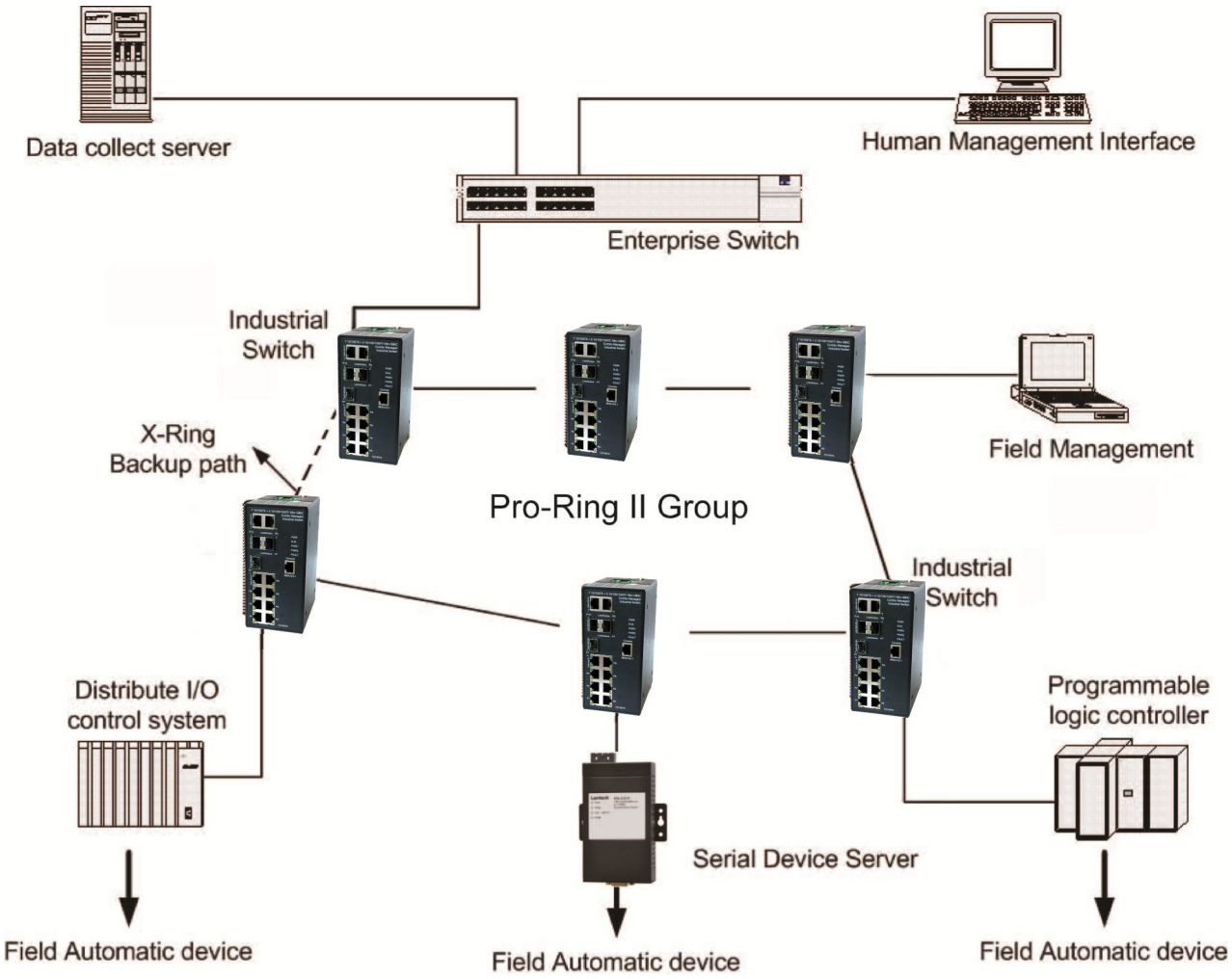
Network Application

This chapter provides some sample applications to help the user to have more actual idea of industrial switch function application. A sample application of the industrial switch is shown as below:



Pro-Ring II Application

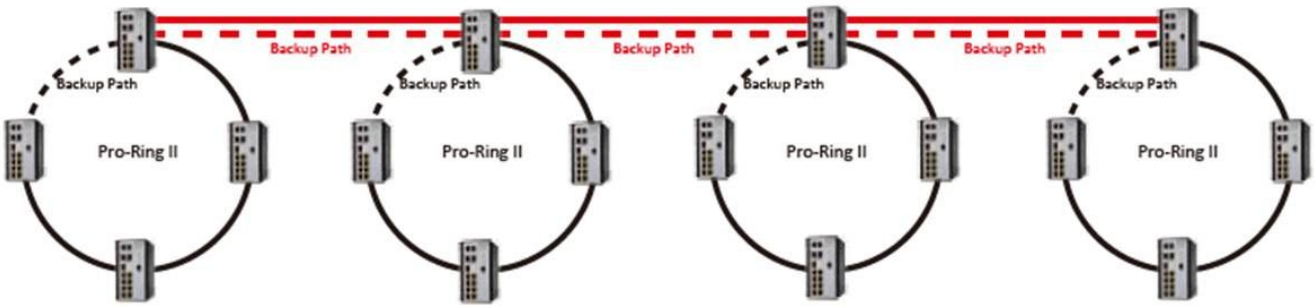
Pro-Ring II is a new Ring mechanism for Equitel Industrial Switches in which it eliminates the need to pre-set the Master switch in old Pro-Ring and yet to protect the network by much secure topologies than ever. Pro-Ring II works as a Ring Chain to reduce the risk of master switch linking down whereas the setup becomes much easier. Pro-Ring II can be backward compatible with old Pro-Ring by down-grading the Ring scheme to old one.



Daisy-Couple Ring

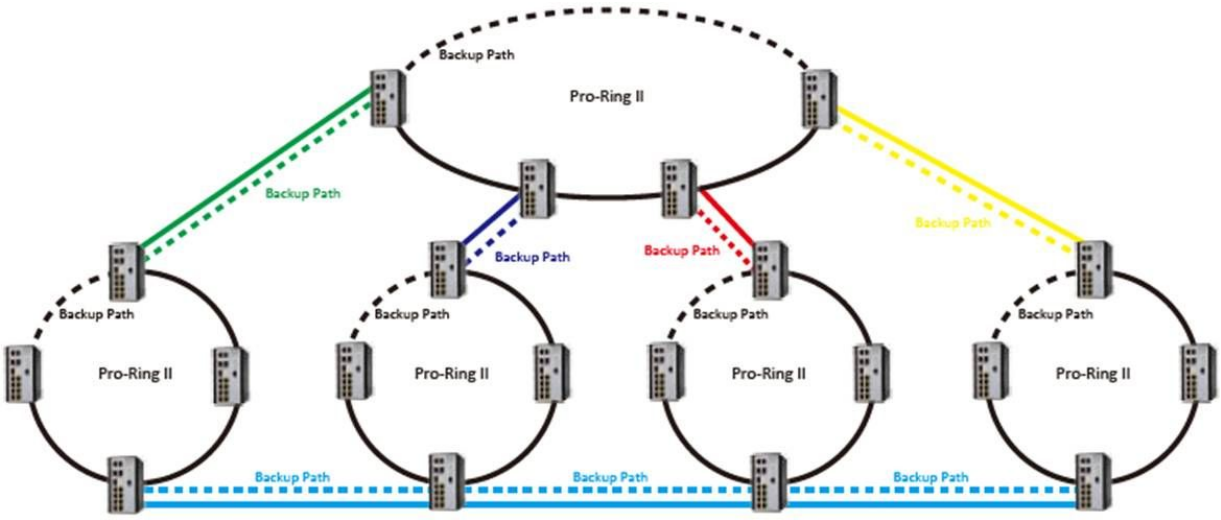
For larger and single LAN group, Daisy-Couple Ring could achieve self-recovery time in

less than 10ms in which the ring group will choose automatically for Master switch, detect loop and form path recovery architecture.



Multi-Couple Ring

For multiple ring groups, it helps to structure ring activities among different LANs. Each ring group has more than 3 redundant paths for backup.

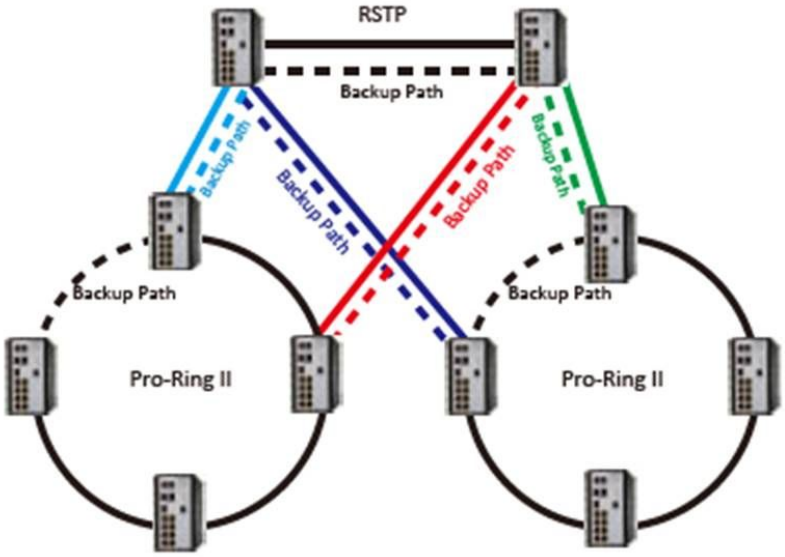


Advanced Dual Homing

When the ring group is connected to upper switch by RSTP algorithm, it strengths the uplink connection with its own redundant path which double secures the link than of

traditional Dual Homing.

[NOTE] In Advanced Dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol.



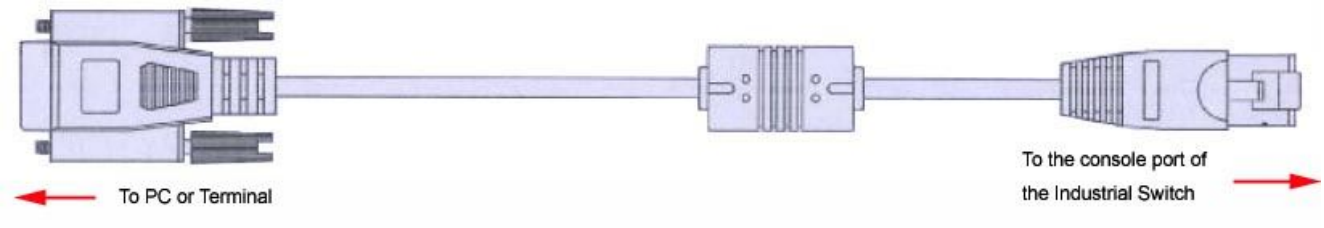
X-Ring II Recovery time table	X-Ring2	Daisy Couple Ring	Multi-Couple Ring	Advance Dual Homing
Recovery Time(ms) (Using 1G Fiber Cable or 100Mb Copper Cable)	10ms	10ms	10ms	Ring Port 10ms, Dual Homing Port 300s
Recovery Time(ms) (Using 1G Copper Cable)	10ms	10ms	10ms	Ring Port 10ms, Dual Homing Port 300s

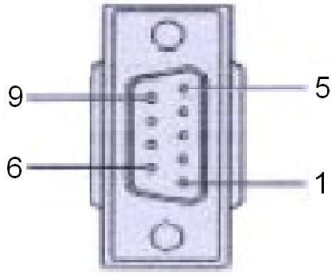
Console Management

Connecting to the Console Port

The supplied cable which one end is RS-232 connector and the other end is RJ-45

connector. Attach the end of RS-232 connector to PC or terminal and the other end of RJ-45 connector to the console port of the switch. The connected terminal or PC must support the terminal emulation program.





DB 9-pin Female

Pin Assignment

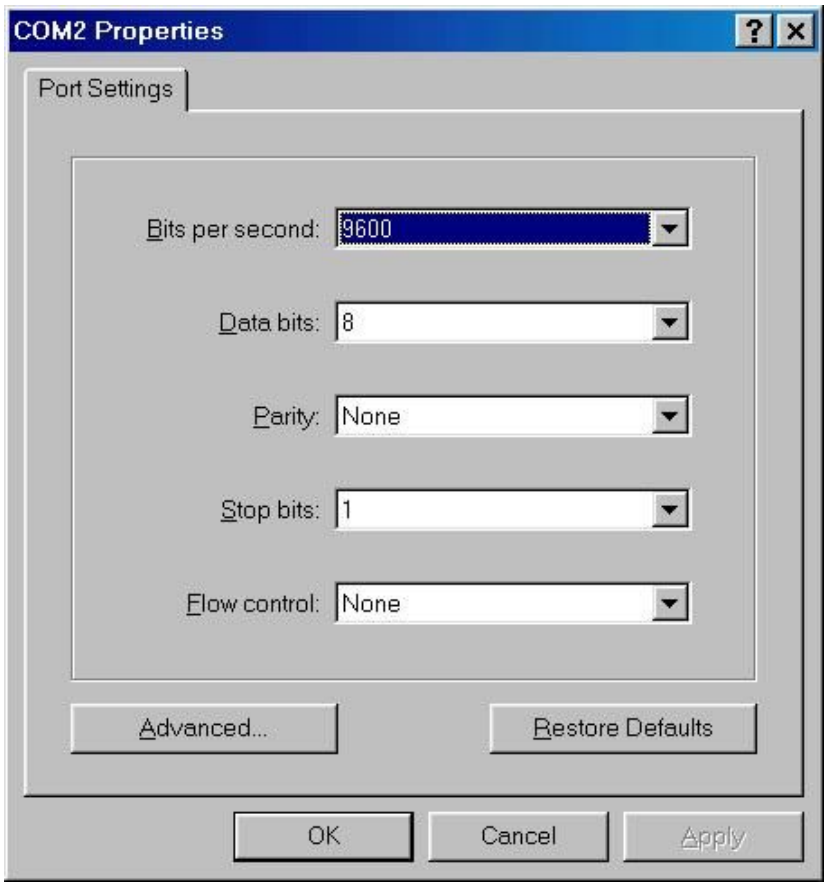
DB9 Connector	RJ-45 Connector
NC	1 Orange/White
2	2 Orange
3	3 Green/White
NC	4 Blue
5	5 Blue/White
NC	6 Green
NC	7 Brown/White
NC	8 Brown

Login in the Console Interface

When the connection between Switch and PC is ready, turn on the PC and run a

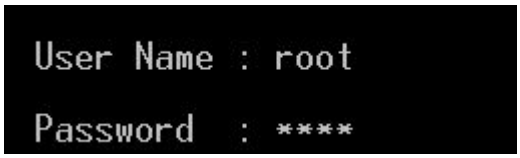
terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



The settings of communication parameters

After finishing the parameter settings, click '**OK'** button. When the blank screen shows up, press **Enter** key to bring out the login prompt. Key in '**root**' (default value) for both User name and Password (use **Enter** key to switch), then press **Enter** key and the Main Menu of console management appears.



Console login interface

CLI Management

The system supports the console management—CLI command. After you log in on to the system, you will see a command prompt. To enter CLI management interface, type in "**enable**" command.

CLI command interface

The following table lists the CLI commands and description.

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user commands available at the user level are a subset of those available at the privileged level.

				Use this mode to • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command while in User EXEC mode.	switch#	Enter **disable** to exit.	The privileged command is the advanced mode. Use this mode to • Display advanced function status • Save configuration
Global Configuration	Enter the **configure** command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure those parameters that are going to be applied to your switch.
VLAN database	Enter the **vlan database** command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface of fast Ethernet command (with a	switch (config-if)#	To exit to global configuration mode, enter **exit**.	Use this mode to configure parameters for the switch and Ethernet ports.

	specific interface) while in global configuration mode		To exit to privileged EXEC mode, enter **exit** or **end**.	

Commands Set List

User EXEC	**E**
Privileged EXEC	**P**
Global configuration	**G**
VLAN database	**V**
Interface configuration	**I**

System Commands Set

Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>**show config**
show terminal	**P**	Show console information	switch#**show terminal**
write memory	**P**	Save user configuration into permanent memory (flash rom)	switch#**write memory**
system name [System Name]	**G**	Configure system name	switch(config)#**system name xxx**
system location [System Location]	**G**	Set switch system location string	switch(config)#**system location xxx**
system description	**G**	Set switch system	switch(config)#**system**

[System Description]		description string	**description xxx**
system contact [System Contact]	**G**	Set switch system contact window string	switch(config)#**system contact xxx**
show system-info	**E**	Show system information	switch>**show system-info**
ip address [Ip-address] [Subnet-mask] [Gateway]	**G**	Configure the IP address of switch	switch(config)#**ip address 192.168.1.1 255.255.255.0 192.168.1.254**
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#**ip dhcp**
show ip	**P**	Show IP information of switch	switch#**show ip**
no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)#**no ip dhcp**
reload	**G**	Halt and perform a cold restart	switch(config)#**reload**
default	**G**	Restore to default	switch(config)#**default**
admin username [Username]	**G**	Changes a login username. (maximum 10 words)	switch(config)#**admin username xxxxxx**
admin password [Password]	**G**	Specifies a password (maximum 10 words)	switch(config)#**admin password xxxxxx**
show admin	**P**	Show administrator information	switch#**show admin**
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#**dhcpserver enable**
Dhcpserver disable	**G**	Disable DHCP Server	switch(config)#**no dhcpserver**
dhcpserver lowip [Low IP]	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip [High IP]	**G**	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.200**

dhcpserver subnetmask [Subnet mask]	**G**	Configure subnet mask for DHCP clients	switch(config)#**dhcpserver subnetmask 255.255.255.0**
dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch(config)#**dhcpserver gateway 192.168.1.254**
dhcpserver dnsip [DNS IP]	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.1.1**
dhcpserver leasetime [Hours]	**G**	Configure lease time (in hour)	switch(config)#**dhcpserver leasetime 1**
dhcpserver ipbinding [IP address]	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**
security ip [Index(1..10)] [IP	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**

Address]			
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**

Port Commands Set

Commands	Level	Description	Example
interface fastEthernet **[Portid]**	**G**	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
duplex **[full | half]**	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed **[10|100|1000|auto]**	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**

no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#**no flowcontrol**
security enable	**I**	Enable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**security enable**
no security	**I**	Disable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**no security**
bandwidth type all	**I**	Set interface ingress limit frame type to “accept all frame”	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type all**
bandwidth type broadcast-multicast-flooded-unicast	**I**	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast-flooded-unicast**
bandwidth type broadcast-multicast	**I**	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast**
bandwidth type broadcast-only	**I**	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-only**
bandwidth in [Value]	**I**	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 100**

		or to 256000 kbps for giga ports, and zero means no limit.	
bandwidth out **[Value]**		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth out 100**
show bandwidth	**I**	Show interfaces bandwidth control	switch(config)#**interface fastEthernet 2** switch(config-if)#**show bandwidth**
state **[Enable | Disable]**	**I**	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#**interface fastEthernet 2** (config-if)#**state Disable**
show interface configuration	**I**	show interface configuration status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface configuration**
show interface status	**I**	show interface actual status	switch(config)#**interface fastEthernet 2** (config-if)#**show interface status**

show interface accounting	**I**	show interface statistic counter	switch(config)#**interface fastEthernet 2** (config-if)#**show interface accounting**
no accounting	**I**	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**

Trunk Commands Set

Commands	Level	Description	Example
aggregator priority [1~65535]	**G**	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport [Group ID] [Port Numbers]	**G**	Set activity port	switch(config)#**aggregator activityport 2**
aggregator group [GroupID] [Port-list] **lacp workp** [Workport]	**G**	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**

		of member ports.	
aggregator group **[GroupID] [Port-list]** **nolacp**	**G**	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**
show aggregator	**P**	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp **[GroupID]**	**G**	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**
no aggregator group **[GroupID]**	**G**	Remove a trunk group	switch(config)#**no aggreator group 2**

VLAN Commands Set

Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**

no vlan	**V**	No VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based **grpname** **[Group Name]** **grpid** **[GroupID]** **port** **[PortNumbers]**	**V**	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group **[GroupID]**	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name **[GroupName]** **vid** **[VID]**	**V**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port **[PortNumber]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 access-link untag 33**
vlan 8021q port **[PortNumber]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**

vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber] **access-link untag** [UntaggedVID]	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**
vlan 8021q trunk [PortNumber] **trunk-link tag** [TaggedVID List]	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**

Spanning Tree Commands Set

Commands	Level	Description	Example
spanning-tree enable	**G**	Enable spanning tree	switch(config)#**spanning-tree enable**
spanning-tree priority [0~61440]	**G**	Configure spanning tree priority parameter	switch(config)#**spanning-tree priority 32767**

spanning-tree max-age [seconds]	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)#**spanning-tree max-age 15**
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the	switch(config)#**spanning-tree forward-time 20**

		specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	
stp-path-cost **[1~200000000]**	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**
stp-path-priority **[Port Priority]**	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 128**

		position as the root switch.	
stp-admin-p2p **[Auto|True|False]**	**I**	Admin P2P of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-p2p Auto**
stp-admin-edge **[True|False]**	**I**	Admin Edge of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-edge True**
stp-admin-non-stp **[True|False]**	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	**E**	Displays a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#**no spanning-tree**

QOS Commands Set

Commands	Level	Description	Example
qos policy **[weighted-fair|strict]**	**G**	Select QOS policy scheduling	switch(config)#**qos policy weighted-fair**
qos prioritytype **[port-based|cos-only|tos-only|cos-first|tos-first]**	**G**	Setting of QOS priority type	switch(config)#**qos prioritytype**
qos priority portbased **[Port]**	**G**	Configure Port-based Priority	switch(config)#**qos priority portbased 1 low**

[lowest|low|middle|high]			
qos priority cos [Priority][lowest|low|middle|high]	**G**	Configure COS Priority	switch(config)#**qos priority cos 0 middle**
qos priority tos [Priority][lowest|low|middle|high]	**G**	Configure TOS Priority	switch(config)#**qos priority tos 3 high**
show qos	**P**	Displays the information of QoS configuration	Switch#**show qos**
no qos	**G**	Disable QoS function	switch(config)#**no qos**

IGMP/MLD Commands Set

Commands	Level	Description	Example
Igmp/mld enable	**G**	Enable IGMP snooping function	switch(config)#**igmp enable**
Igmp/mld -query auto	**G**	Set IGMP query to auto mode	switch(config)#**Igmp-query auto**
Igmp/mld -query force	**G**	Set IGMP query to force mode	switch(config)#**Igmp-query force**
show igmp/mld configuration	**P**	Displays the details of an IGMP configuration.	switch#**show igmp configuration**
show igmp/mld multi	**P**	Displays the details of an IGMP snooping entries.	switch#**show igmp multi**
no igmp/mld	**G**	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp/mld -query	**G**	Disable IGMP query	switch#**no igmp-query**

Mac / Filter Table Commands Set

Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)#**interface fastEthernet 2** switch(config-if)#**mac-address-table static hwaddr 000012345678**
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#**mac-address-table filter hwaddr 000012348678**
show mac-address-table	P	Show all MAC address table	switch#**show mac-address-table**
show mac-address-table static	P	Show static MAC address table	switch#**show mac-address-table static**
show mac-address-table filter	P	Show filter MAC address table.	switch#**show mac-address-table filter**
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#**interface fastEthernet 2** switch(config-if)#**no mac-address-table static hwaddr 000012345678**
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#**no mac-address-table filter hwaddr 000012348678**
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#**no mac-address-table**

SNMP Commands Set

Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings [Community] **right** [RO/RW]	G	Add SNMP community string.	switch(config)#**snmp community-strings public right rw**
snmp-server host [IP address] **community** [Community-string] **trap-version** [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#**snmp-server host 192.168.1.50 community public trap-version v1 (remove)** Switch(config)# **no snmp-server host 192.168.1.50**
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#**snmpv3 context-name Test**
snmpv3 user [User Name] **group** [Group Name] **password** [Authentication	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**

Password] [Privacy Password]			
snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**G**	Configure the access table of SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Configure the mibview table of SNMPV3 agent	switch(config)#**snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**
show snmp	**P**	Show SNMP configuration	switch#**show snmp**
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)#**no snmp community-strings public**
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)#**no snmp-server 192.168.1.50**
no snmpv3 user [User Name]	**G**	Remove specified user of SNMPv3	switch(config)#**no snmpv3 user Test**

		agent.	
no snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1**
no snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

Port Mirroring Commands Set

Commands	Level	Description	Example
monitor [RX|TX|Both]	**I**	Configure source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**monitor RX**
monitor rx [Port ID]	**G**	Set RX destination	switch(config)#**monitor rx 2**

		port of monitor function	
monitor tx [Port ID]	**G**	Set TX destination port of monitor function	switch(config)#**monitor tx 3**
show monitor	**P**	Show port monitor information	switch#**show monitor**
show monitor	**I**	Show port monitor information	switch(config)#**interface fastEthernet 2** switch(config-if)#**show monitor**
no monitor	**I**	Disable source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**no monitor**

802.1x Commands Set

Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# **8021x enable**
8021x system radiusip [IP address]	**G**	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# **8021x system radiusip 192.168.1.1**
8021x system serverport [port ID]	**G**	Use the 802.1x system server port global configuration command to change	switch(config)# **8021x system serverport 1815**

		the radius server port	
8021x system accountport [port ID]	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# **8021x system accountport 1816**
8021x system sharekey [ID]	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system sharekey 123456**
8021x system nasid [words]	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# **8021x system nasid test1**
8021x misc quietperiod [sec.]	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# **8021x misc txperiod 5**
8021x misc supportimeout [sec.]	**G**	Use the 802.1x misc supp timeout global	switch(config)# **8021x misc supportimeout 20**

		configuration command to set the supplicant timeout.	
8021x misc servertimeout [sec.]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# **8021x misc maxrequest 3**
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# **8021x misc reauthperiod 3000**
8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#**interface fastethernet 3** switch(config-if)#**8021x portstate accept**
show 8021x	**E**	Displays a summary of the 802.1x properties and also the port sates.	switch>**show 8021x**
no 8021x	**G**	Disable 802.1x	switch(config)#**no 8021x**

		function	

TFTP Commands Set

Commands	Level	Description	Defaults Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**backup flash:backup_cfg**
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#**restore flash:restore_cfg**
upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**upgrade lash:upgrade_fw**

SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
systemlog ip [IP address]	**G**	Set System log server IP address.	switch(config)# **systemlog ip 192.168.1.100**
systemlog mode [client|server|both]	**G**	Specified the log mode	switch(config)# **systemlog mode both**
show systemlog	**E**	Displays system log.	Switch>**show systemlog**
show systemlog	**P**	Show system log client & server	switch#**show systemlog**

		information	
no systemlog	**G**	Disable systemlog functon	switch(config)#**no systemlog**
smtp enable	**G**	Enable SMTP function	switch(config)#**smtp enable**
smtp serverip **[IP address]**	**G**	Configure SMTP server IP	switch(config)#**smtp serverip 192.168.1.5**
smtp authentication	**G**	Enable SMTP authentication	switch(config)#**smtp authentication**
smtp account **[account]**	**G**	Configure authentication account	switch(config)#**smtp account John**
smtp password **[password]**	**G**	Configure authentication password	switch(config)#**smtp password 1234**
smtp rcptemail **[Index] [Email address]**	**G**	Configure Rcpt e-mail Address	switch(config)#**smtp rcptemail 1 Alert@test.com**
show smtp	**P**	Show the information of SMTP	switch#**show smtp**
no smtp	**G**	Disable SMTP function	switch(config)#**no smtp**
event device-cold-start **[Systemlog|SMTP|Both]**	**G**	Set cold start event type	switch(config)#**event device-cold-start both**
event authentication-failure **[Systemlog|SMTP|Both]**	**G**	Set Authentication failure event type	switch(config)#**event authentication-failure both**
event systemlog **[Link-UP|Link-Down|Both]**	**I**	Set port event for system log	switch(config)#**interface fastethernet 3** switch(config-if)#**event systemlog both**
event smtp	**I**	Set port event for	switch(config)#**interface**

[Link-UP|Link-Down|Both]		SMTP	**fastethernet 3** switch(config-if)#**event smtp both**
show event	**P**	Show event selection	switch#**show event**
no event device-cold-start	**G**	Disable cold start event type	switch(config)#**no event device-cold-start**
no event authentication-failure	**G**	Disable Authentication failure event typ	switch(config)#**no event authentication-failure**
no event systemlog	**I**	Disable port event for system log	switch(config)#**interface fastethernet 3** switch(config-if)#**no event systemlog**
no event smpt	**I**	Disable port event for SMTP	switch(config)#**interface fastethernet 3** switch(config-if)#**no event smtp**
show systemlog	**P**	Show system log client & server information	switch#**show systemlog**

SNTP Commands Set

Commands	Level	Description	Example
sntp enable	**G**	Enable SNTP function	switch(config)#**sntp enable**
sntp daylight	**G**	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight**
sntp daylight-period [Start time] [End time]	**G**	Set period of daylight saving time, if SNTP function is inactive,	switch(config)# **sntp daylight-period 20060101-01:01 20060202-01:01**

		this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	
sntp daylight-offset **[Minute]**	**G**	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight-offset 3**
sntp ip **[IP]**	**G**	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp ip 192.169.1.1**
sntp timezone **[Timezone]**	**G**	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#**sntp timezone 22**
show sntp	**P**	Show SNTP information	switch#**show sntp**
show sntp timezone	**P**	Show index number of time zone list	switch#**show sntp timezone**
no sntp	**G**	Disable SNTP function	switch(config)#**no sntp**
no sntp daylight	**G**	Disable daylight saving time	switch(config)#**no sntp daylight**

Pro-ring II Commands Set

Commands	Level	Description	Example
ring2 mode enable [X-Ring2|Legacy-Ring]	G	Enable X-ring2 mode	switch(config)#**ring2 mode [X-Ring2|Legacy-Ring]**
ring2 add [Ring ID][1st Ring Port][2nd Ring Port][1st Rdn Port][1st Rdn Port ID][2nd Rdn Port][2nd Rdn Port ID]	G	Add X-Ring2 entry	switch(config)#**ring2 add 1 1 2 3 2 4 2**
ring2 del [Index]	G	Delete X-Ring2 entry	switch(config)#**ring2 del 1**
ring2 show	G	Show X-Ring2 configuration	switch(config)#**ring2 show**
ring2 ringport [1st Ring Port] [2nd Ring Port]	G	Configure Legacy-Ring 1st/2nd Ring Port	switch(config)#**ring2 ringport 7 8**

Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

There is an embedded HTML web site residing in flash memory on CPU board of the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0 or later version. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

Preparing for Web Management

Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password are listed as below:

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**

- User Name: **root**
- Password: **root**

System Login

1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as ‘**root**’.
5. Press ‘**Enter**‘ or click **OK** button, and then the home screen of the Web-based management appears.

System Information

Assign the system name and location and view the system information

- **System Name:** Assign the system name of the switch (The maximum length is 64 bytes)
- **System Description:** Describes the switch.
- **System Location:** Assign the switch physical location (The maximum length is 64 bytes).
- **System Contact:** Enter the name of contact person or organization.
- **Firmware Version:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default)
- And than, click button.

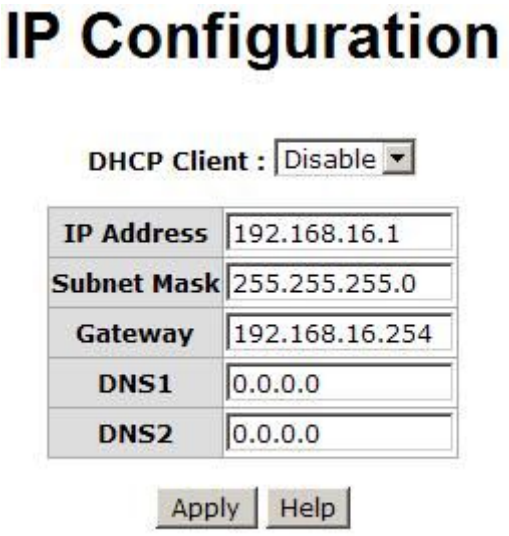
System information interface

IP Configuration

User can configure the IP Settings and DHCP client function in here.

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the industrial switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After user click **Apply** button, a popup dialog shows up. It is to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabled, and then the user doesn't need to assign the IP address. And, the network DHCP server will assign the IP address displaying in this column for the industrial switch. The default IP is 192.168.16.1.
- **Subnet Mask:** Assign the subnet mask to the IP address. If DHCP client function is enabled, and then the user does not need to assign the subnet mask.
- **Gateway:** Assign the network gateway for the industrial switch. The default gateway is 192.168.16.254.

- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, click Apply



IP configuration interface

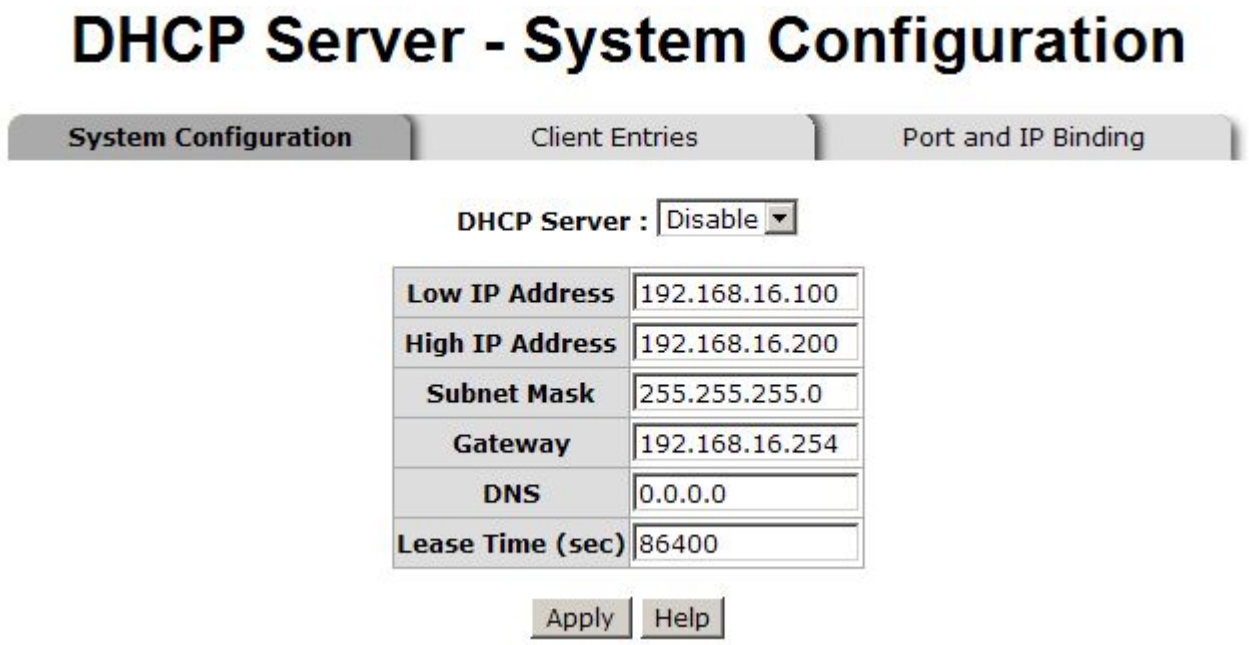
DHCP Server – System configuration

DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.

- **Low IP Address:** Type in an IP address. Low IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP address.
- **High IP Address:** Type in an IP address. High IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.200 is the High IP address.
- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, click Apply



DHCP Server Configuration interface

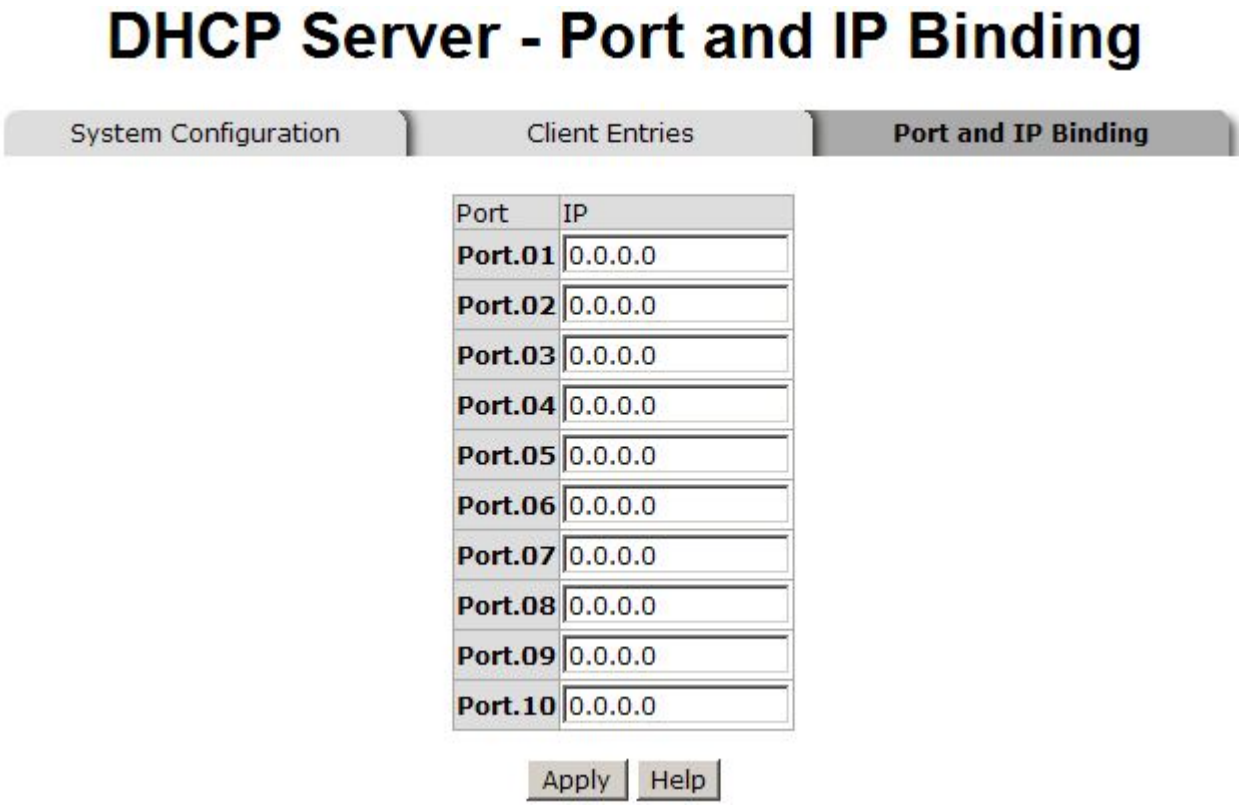
DHCP Server – Client Entries

When the DHCP server function is active, the system will collect the DHCP client information and displays it at this tab.

DHCP Client Entries interface

DHCP Server - Port and IP Bindings

Assign the dynamic IP address to the port. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address that has been assigned before to the connected device.

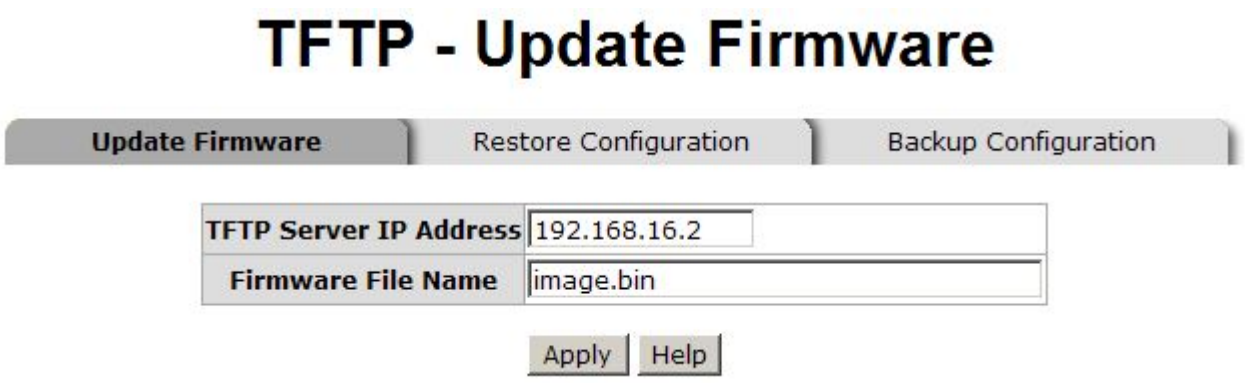


Port and IP Bindings interface

TFTP - Update Firmware

It provides the functions that allow user to update the switch firmware. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

1. **TFTP Server IP Address:** Type in your TFTP server IP.
2. **Firmware File Name:** Type in the name of firmware image.
3. Click Apply.



Update Firmware interface

TFTP – Restore Configuration

You can restore the configuration from TFTP server. Before doing that, you must put the image file on TFTP server first and the switch will download back the flash image.

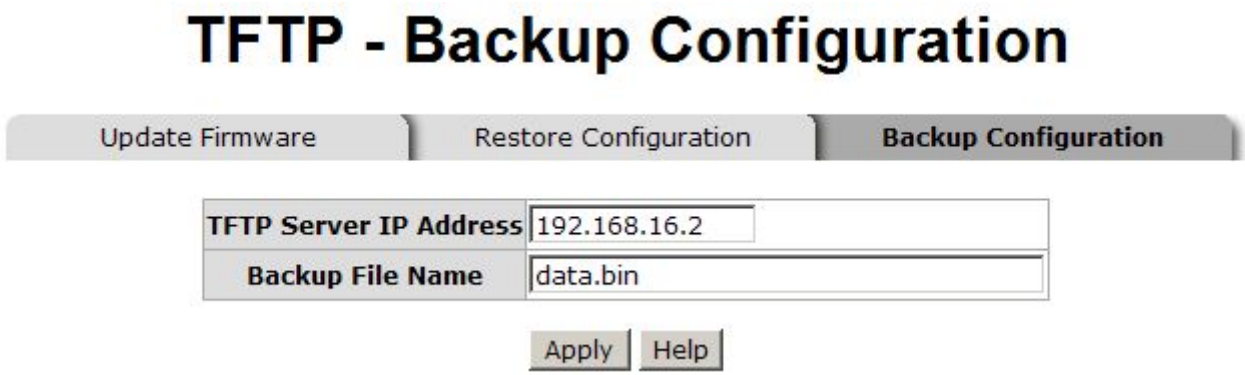
1. **TFTP Server IP Address:** Type in the TFTP server IP.
2. **Restore File Name:** Type in the correct file name for restoring.
3. Click Apply.

Restore Configuration interface

TFTP - Backup Configuration

You can save the current configuration from flash ROM to TFTP server for restoring later.

1. **TFTP Server IP Address:** Type in the TFTP server IP.
2. **Backup File Name:** Type in the file name.
3. Click Apply.

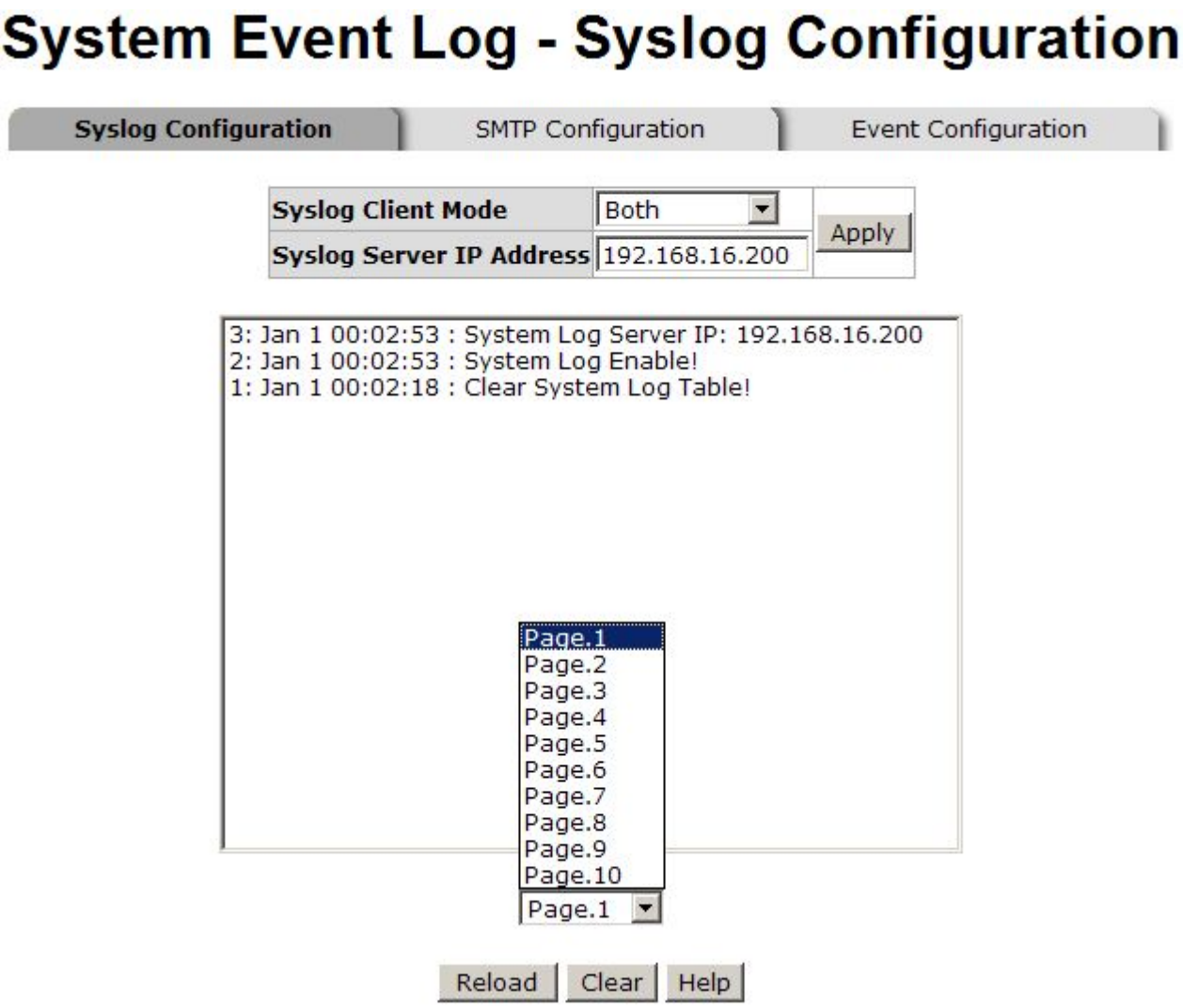


Backup Configuration interface

System Event Log – Syslog Configuration

Configure the system event mode to collect system log.

1. **Syslog Client Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**.
2. **System Log Server IP Address:** Assign the system log server IP.
3. When Syslog Client Mode is set as **Client Only**, the system event log will only be sent to the client which has logged in on the switch. When Syslog Client Mode is set as **Server Only**, the system log will only be sent to the syslog server and you have to type the IP address in the Sysylog Server IP Address column. If the Syslog Client Mode is set as **Both**, the system log will be sent to client and server.
4. Click Reload to refresh the events log.
5. Click Clear to clear all current events log.
5. After configuring, Click Apply.



Syslog Configuration interface

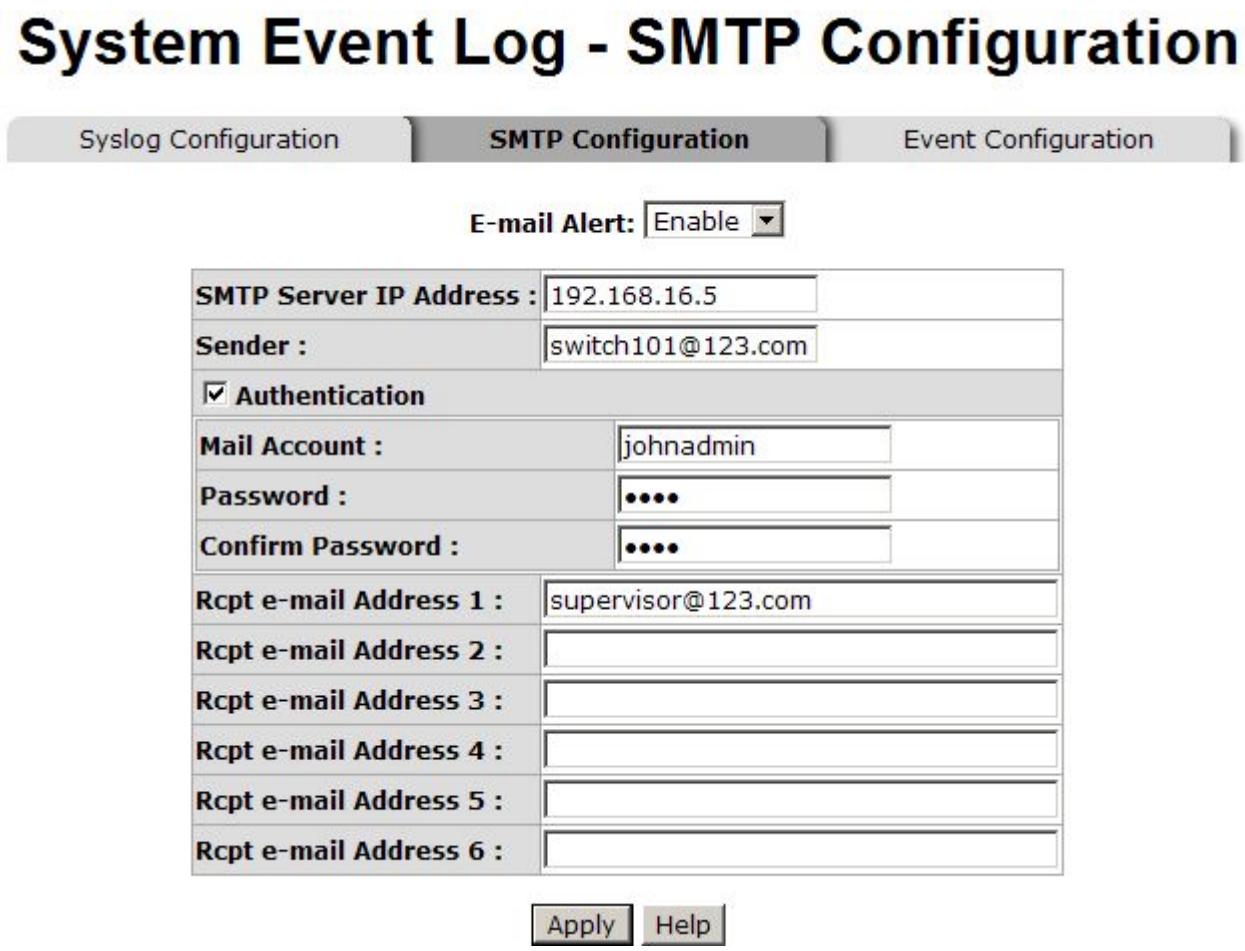
System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, password, and forwarded email account for receiving the event alert.

1. **Email Alert:** Enable or disable the email alert function.
2. **SMTP Server IP:** Set up the mail server IP address (when **Email Alert** enabled, this function will then be available).
3. **Sender:** Type in an alias of the switch in complete email address format, e.g.

switch101@123.com, to identify where the event log comes from.

4. **Authentication:** Tick the checkbox to enable this function, configuring the email account and password for authentication (when **Email Alert** enabled, this function will then be available).
5. **Mail Account:** Set up the email account, e.g. johnadmin, to receive the alert. It must be an existing email account on the mail server, which you had set up in **SMTP Server IP Address** column.
6. **Password:** Type in the password to the email account.
7. **Confirm Password:** Reconfirm the password.
8. **Rcpt e-mail Address 1 ~ 6:** You can also assign up to 6 e-mail accounts to receive the alert.
9. Click Apply button.



SMTP Configuration interface

System Event Log - Event Configuration

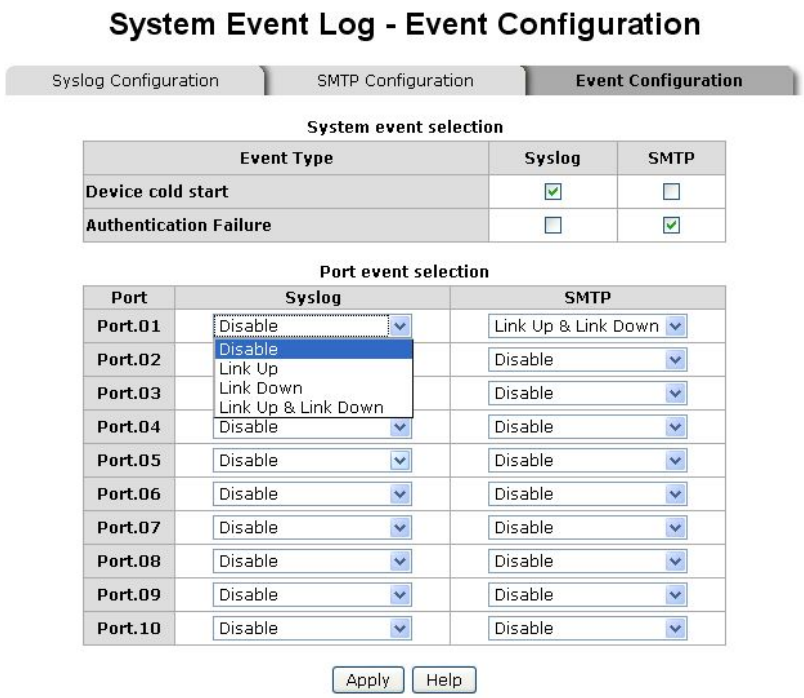
When the **Syslog/SMTP** checkbox is marked, the event log will be sent to system log server/SMTP server. Also, per port log (link up, link down, and both) events can be sent to the system log server/SMTP server with the respective checkbox ticked. After configuring, click Apply to have the setting taken effect.

- **System event selection:** There are 2 event types—Device cold start and Authentication Failure. Before you can tick the checkbox of each event type, the Syslog Client Mode column on the Syslog Configuration tab/E-mail Alert column on

the SMTP Configuration tab must be enabled first.

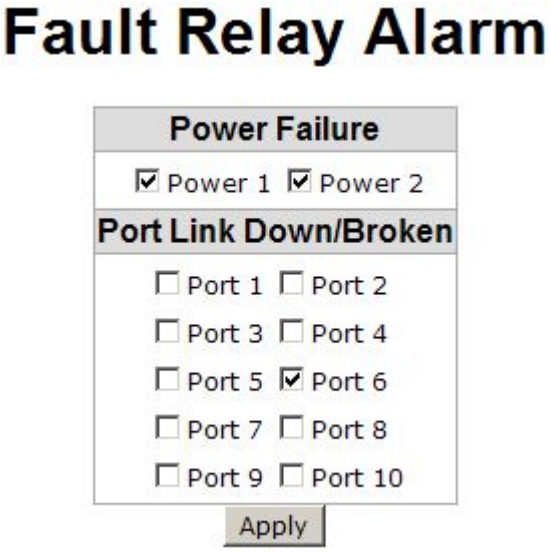
- **Device cold start:** When the device executes cold start action, the system will issue a log event.
- **Authentication Failure:** When the SNMP authentication fails, the system will issue a log event.

- **Port event selection:** Also, before the drop-down menu items are available, the Syslog Client Mode column on the Syslog Configuration tab and the E-mail Alert column on the SMTP Configuration tab must be enabled first. Those drop-down menu items have 3 selections—Link UP, Link Down, and Link UP & Link Down. Disable means no event will be sent to the system log server/SMTP server.
  - **Link UP:** The system will issue a log message when port connection is up only.
  - **Link Down:** The system will issue a log message when port connection is down only.
  - **Link UP & Link Down:** The system will issue a log message when port connection is up and down.



Fault Relay Alarm

- **Power Failure:** Tick the checkbox to enable the function of lighting up the **FAULT** LED on the panel when power fails.
- **Port Link Down/Broken:** Tick the checkbox to enable the function of lighting up **FAULT** LED on the panel when Ports' states are link down or broken.



Fault Relay Alarm interface

SNTP Configuration

You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

1. **SNTP Client:** Enable/disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** Enable/disable daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
3. **UTC Timezone:** Set the switch location time zone. The following table lists the

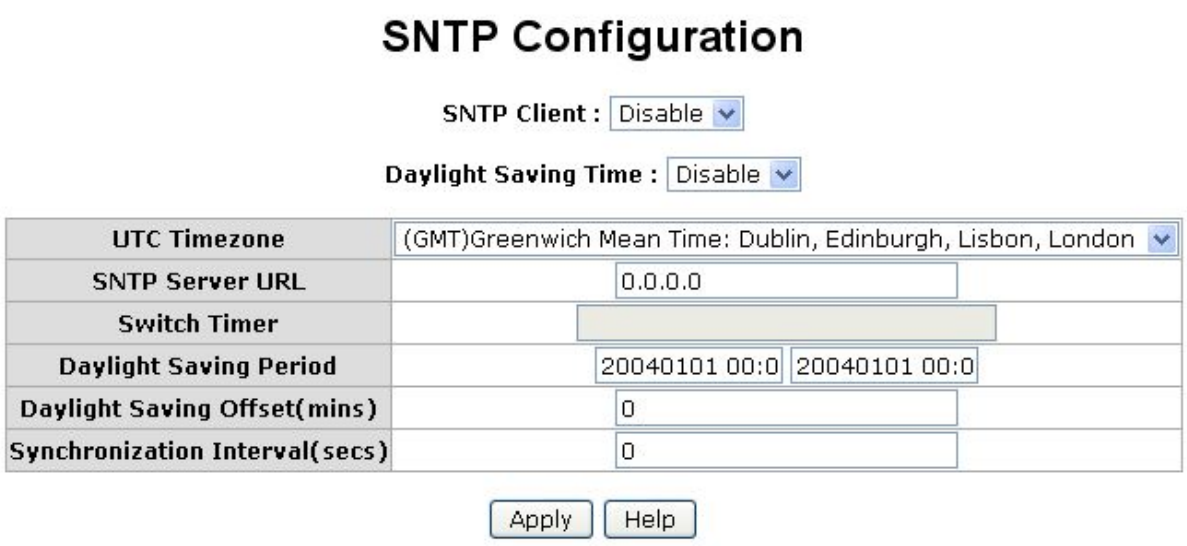
different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am

CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard	+12 hours	Midnight

NZT - New Zealand		

4. **SNTP Sever URL:** Set the SNTP server IP address.
5. **Switch Timer:** Displays the current time of the switch.
6. **Daylight Saving Period:** Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
7. **Daylight Saving Offset (mins):** For non-US and European countries, specify the amount of time for day light savings.
8. **Synchronization Interval(secs):** The Synchronization Interval is used for sending synchronizing packets periodically. User can assign range from 64s to 1024s. The default setting of values is "0" means that you disable the auto synchronizes feature in SNTP client mode. You can enable the feature when filling the interval range from 64s~1024s.
9. Click Apply.



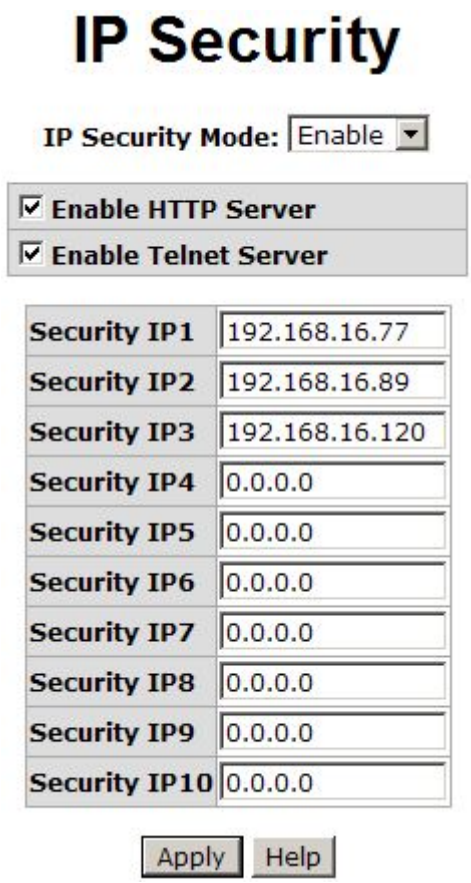
SNTP Configuration interface

IP Security

IP security function allows the user to assign 10 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

- **IP Security Mode:** When this option is in **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** checkboxes will then be available.
- **Enable HTTP Server:** When this checkbox is ticked, the IP addresses among Security IP1 ~ IP10 will be allowed to access this switch via HTTP service.
- **Enable Telnet Server:** When this checkbox is ticked, the IP addresses among Security IP1 ~ IP10 will be allowed to access this switch via telnet service.
- **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only these 10 IP addresses can access and manage the switch through the HTTP/Telnet service.
- And then, click Apply button to apply the configuration.

[NOTE]	Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.



IP Security interface

User Authentication

Change web management login user name and password for the management security issue.

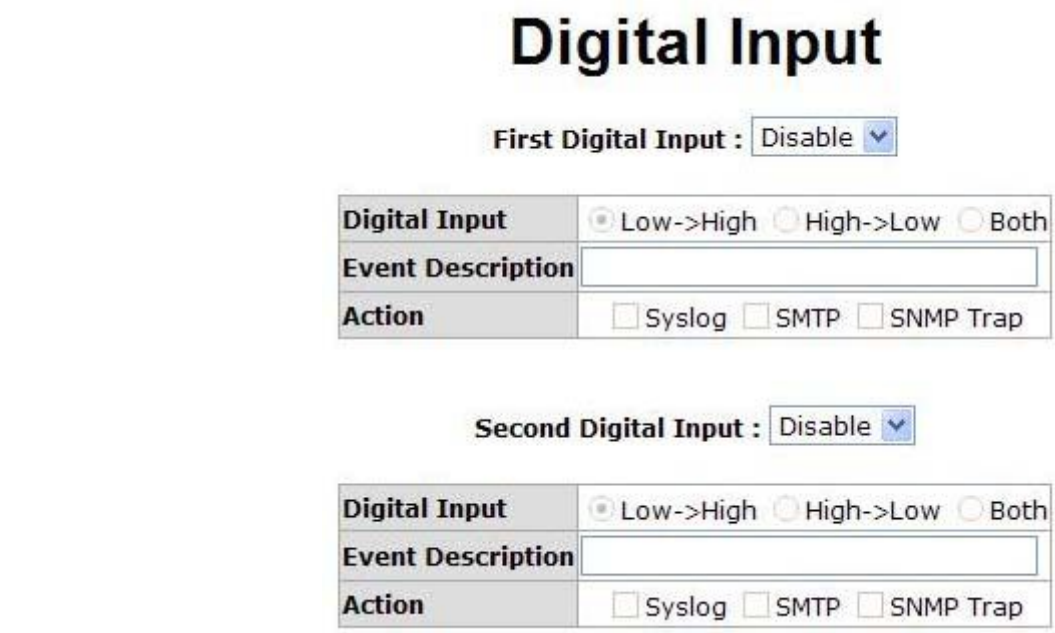
1. **User name:** Type in the new user name (The default is 'root')
2. **Password:** Type in the new password (The default is 'root')
3. **Confirm password:** Re-type the new password
4. And then, click Apply

User Authentication interface

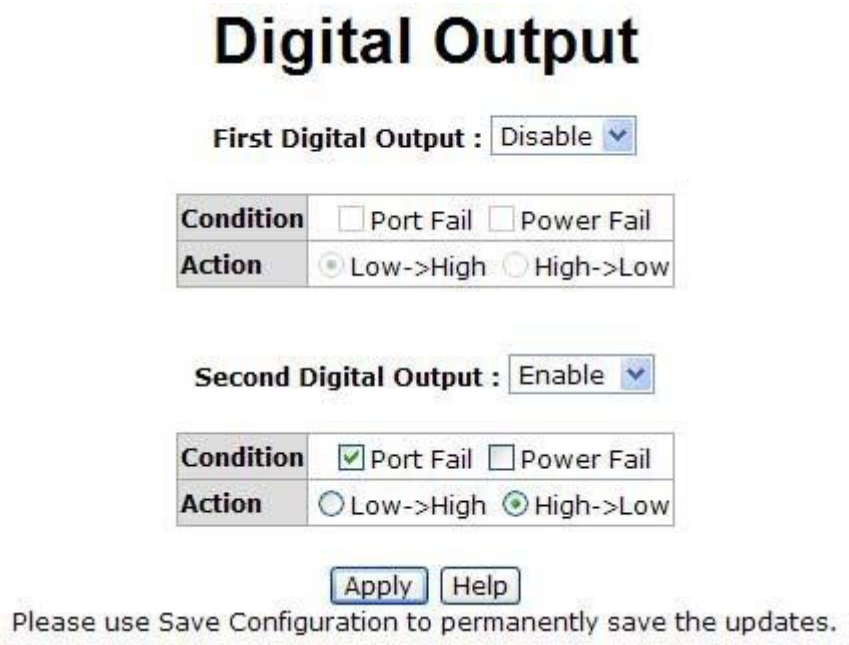
Digital Input/Output

The 7 10/100TX + 3 10/100/1000T/100/1000 SFP Combo w/ X-Ring L2 Managed Industrial Switch contains two digital outputs and two digital inputs. Outputs are open-collector transistor switches that may be controlled by the host computer. They provide messages, which can be applied to heaters, pumps, and other electrical equipment. The digital inputs may be read by the host computer and used to sense the state of a remote digital signal.

- When **First/Second Digital Input** function is enabled, First Digital Input and Second Digital Input will then be available respectively.
- **Digital Input:** Choose the transition type to trigger DI0/DI1.
  - **Low→High:** Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from low to high.
  - **High→Low:** Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from high to low.
- **Event description:** Please fill in the description for the event.
- **Action:** Tick the check boxes to decide whether or not to send the events via Syslog, SMTP, or SNMP Trap.



- When **First/Second Digital Output** function is enabled, First Digital Output and Second Digital Output will then be available respectively.
- **Digital Output:** Choose the transition type to trigger DO0/DO1.
- **Condition:** Please chose the event.
- **Action:**
  - **Low→High:** Having focused this radio button, DO0/DO1 will only report the status when the condition has been triggered then the circuit will be open.\
  - **High→Low:** Having focused this radio button, DO0/DO1 will only report the status when the condition has been triggered then the circuit will be close.



Digital Input/Output interface
*This digital output condition will follow Fault Relay Alarm

Port Statistics

The following information provides the current port statistic information.

- **Port:** Displays the port number.
- **Type:** Displays the media type of the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** The user can set the state of the port as 'Enable' or 'Disable' via Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 bytes], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving good packets (including undersize [less than 64 bytes], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.

- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Click Clear button to clean all counts.

Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Up	Enable	645	0	5957	0	0	2	0	3717	884
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Clear Help

Port Statistics interface

Port Control

In Port control, you can view and set the operation mode of each port.

1. **Port:** Select the port that you want to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port state is set as ‘Disable’, it will not receive or transmit any packet.
3. **Negotiation:** Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to assign the speed and duplex mode manually.
4. **Speed:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read only.
5. **Duplex:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read only.

6. **Flow Control:** Set flow control function as Enable or Disable. When enabled, once the device exceed the input data rate of another device as a result the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
7. **Security:** Once the Security selection is set as '**On**', any access from the device which connects to this port will be blocked unless the MAC address of the device is included in the static MAC address table. See the segment of Static MAC Table.
8. Click Apply button to make the configuration effective.

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.02	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.03	N/A	100TX	Up	Enable	Auto	100 Full	100 Half	Enable	OFF	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.07	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.09	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.10	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Port Control interface

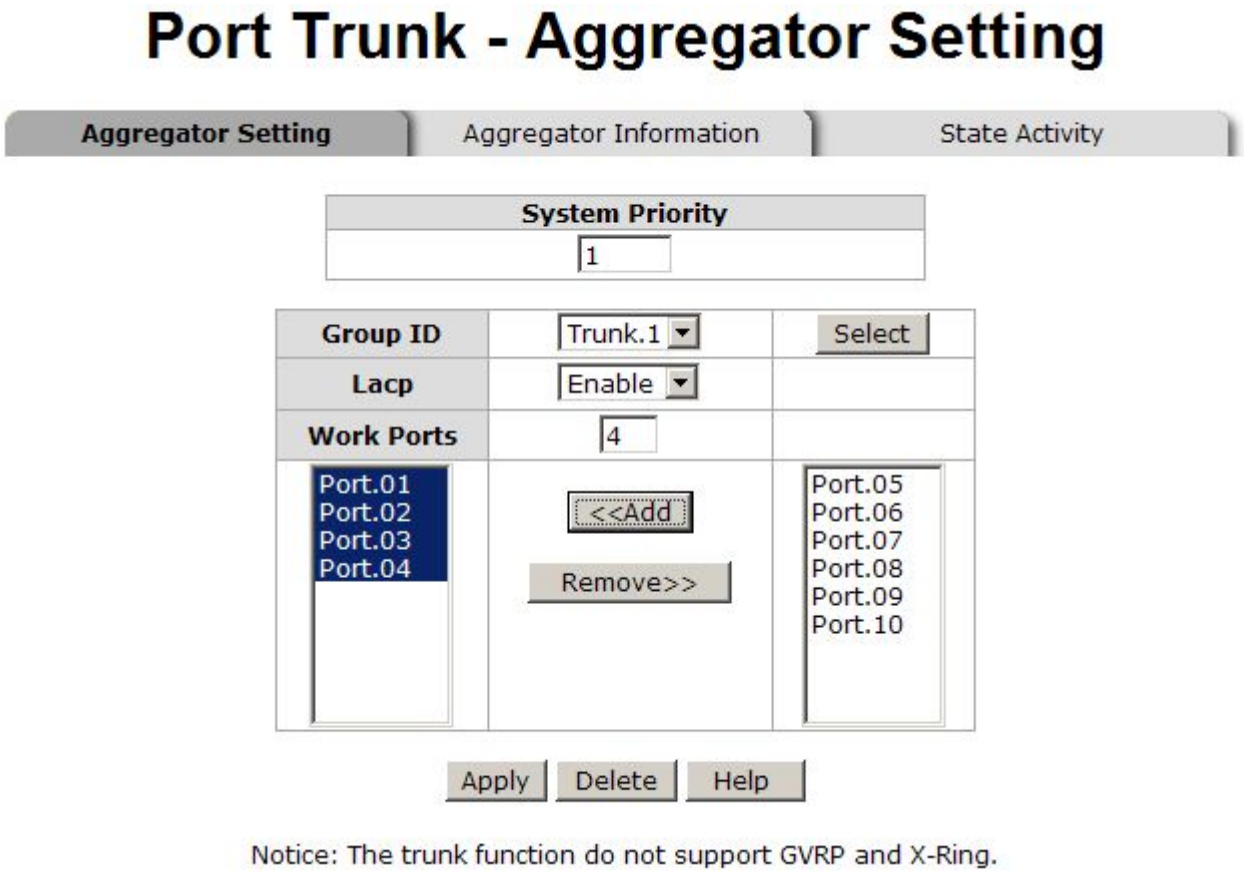
Port Trunk

Port trunk allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing, and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links. Traffic in a trunk is distributed across an individual link within the trunk in a deterministic method that called a hash algorithm. Traffic pattern on the network should be considered carefully before applying it. When a proper hash algorithm is used, traffic is kind of randomly decided to be transmitted across either link within the trunk and load balancing will be seen.

Aggregator setting

1. **System Priority:** A value which is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are four trunk groups to be selected. Choose the "**Group ID**" and click Select button.
3. **LACP:** When enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports. But member ports won't know that they should be aggregated together to form a logic trunk group.
4. **Work ports:** This column field allows the user to type in the total number of active port up to four. With LACP static trunk group, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby (the **LACP State Activity** will show 'Passive' on the tab of **State Activity**) and can be aggregated if work ports fail. If it is a static trunk group, the number of work ports must equal the total number of group member ports.

5. Select the ports to join the trunk group. The system allows four ports maximum to be aggregated in a trunk group. Click Add button to add the port which is focused to the left field. To remove unwanted ports, select the port and click Remove button.
6. When LACP enabled, you can configure LACP Active/Passive status for each port on State Activity page.
7. Click Apply button.
8. Use Delete button to delete Trunk Group. Select the Group ID and click Delete button.

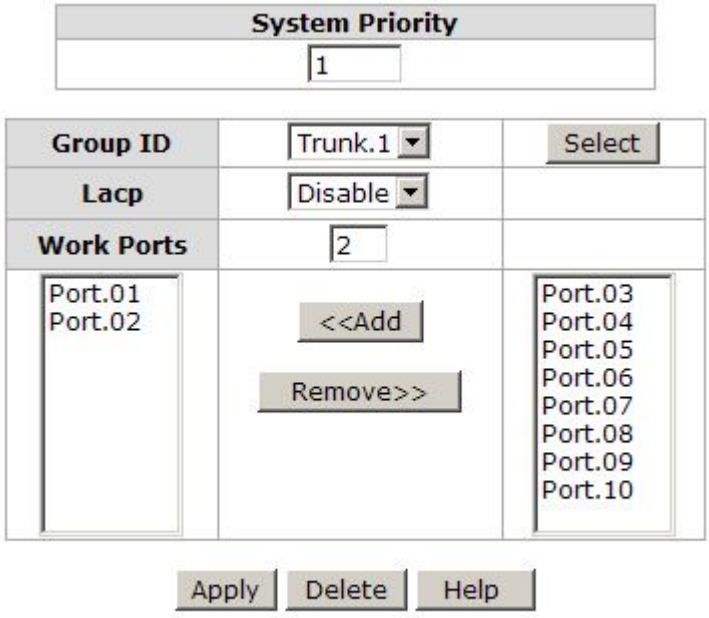


Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

Aggregator Information

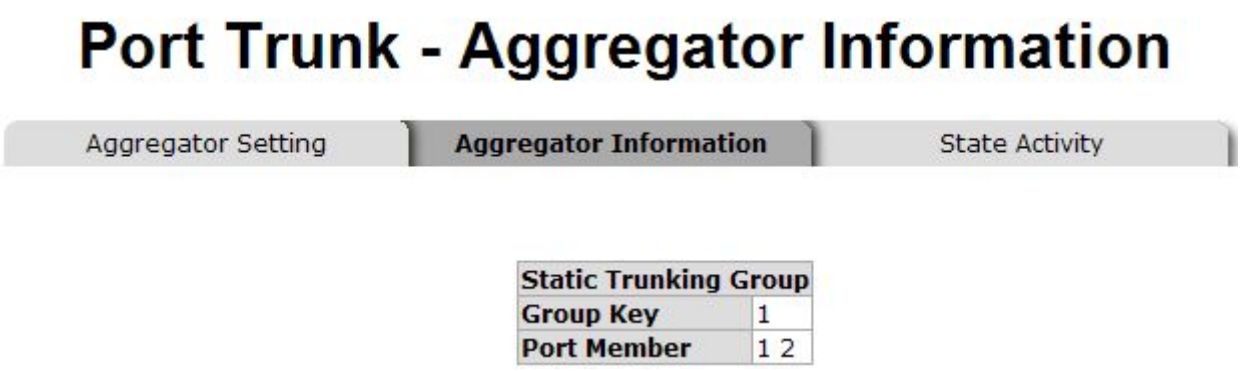
When you have setup the aggregator setting with LACP disabled, you will see the local static trunk group information in here.

1. **Group Key:** Displays the trunk group ID.
2. **Port Member:** Displays the members of this static trunk group.



Notice: The trunk function do not support GVRP and X-Ring.

Port Trunk—Aggregator Setting interface (two ports are added to the left field with LACP disable)



Static Trunking Group	
Group Key	1
Port Member	1 2

Port Trunk – Aggregator Information interface

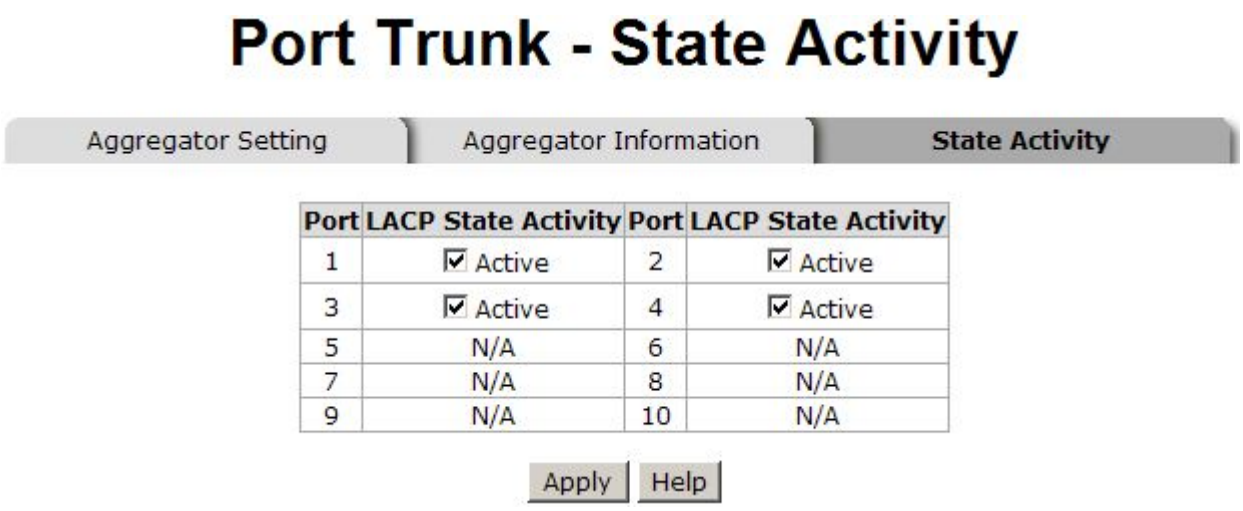
State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state display. When you remove the tick mark to the port and click Apply button, the port state activity will change to **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

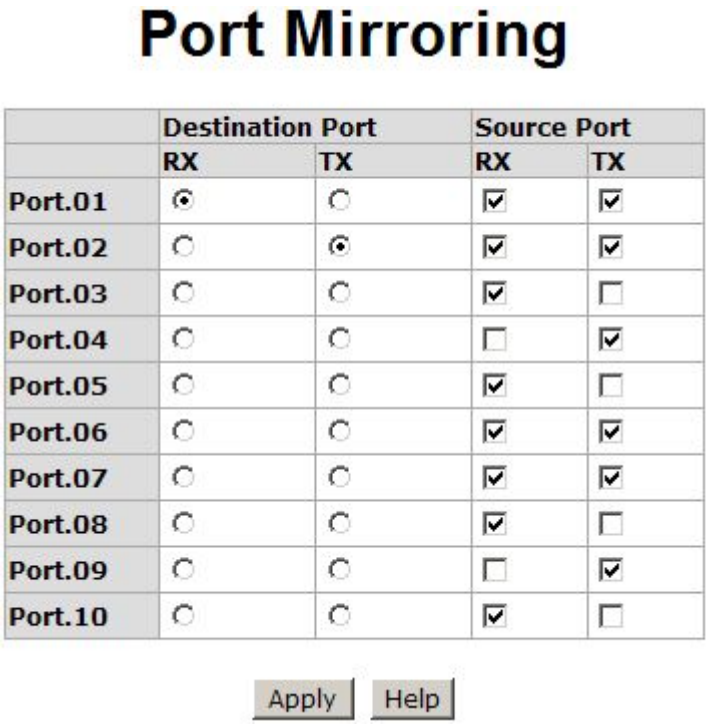
1. **A link** having either two active LACP nodes or one active node can perform dynamic LACP trunk.
2. **A link** having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.



Port Trunk – State Activity interface

Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port which means traffic goes in or out monitored (source) ports will be duplicated into mirroring (destination) port.



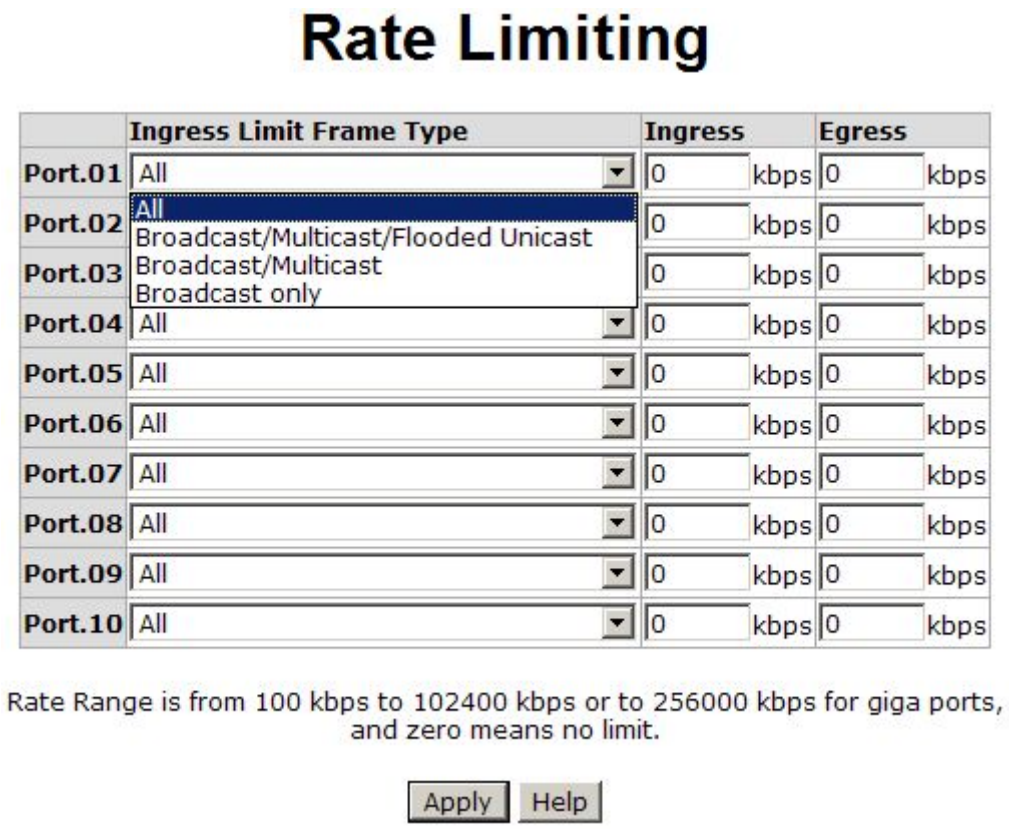
Port Trunk – Port Mirroring interface

- **Destination Port:** There is only one port can be selected to be the destination (mirroring) port for monitoring both RX and TX traffic which come from the source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. The user can connect the mirroring port to LAN analyzer or Netxray.
- **Source Port:** The ports that the user wants to monitor. All monitored port traffic will be copied to mirroring (destination) port. The user can select multiple source ports by ticking the **RX** or **TX** checkboxes to be monitored.

- And then, click Apply button.

Rate Limiting

You can set up every port's frame limitation type and bandwidth rate.



Rate Limiting interface

- **Ingress Limit Frame type:** Select the frame type you want to filter. The frame types have 4 options for selecting: **All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast,** and **Broadcast only**.

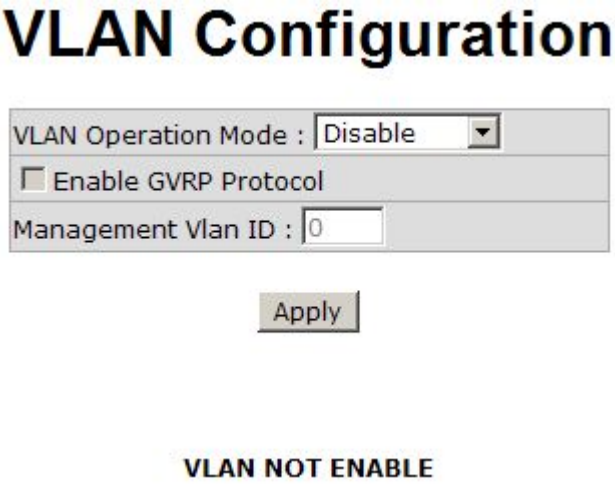
  The four frame type options are for ingress frames limitation. The egress rate only supports '**All**' type.

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps; the user can set the effective egress rate of port 1 as 1Mbps, ingress rate 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate.
  - **Ingress:** Enter the port effective ingress rate (The default value is “0”).
  - **Egress:** Enter the port effective egress rate (The default value is “0”).
- And then, click Apply to make the settings taken effect.

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The switch N967 supports **Port-based** and **802.1Q** (tagged-based) VLAN. The default configuration of VLAN operation mode is “**Disable**”.

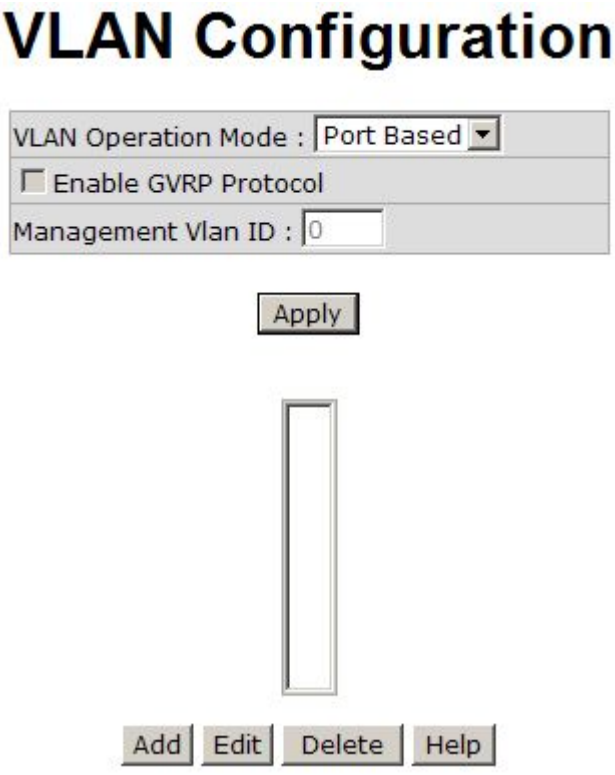


VLAN Configuration interface

VLAN configuration - Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

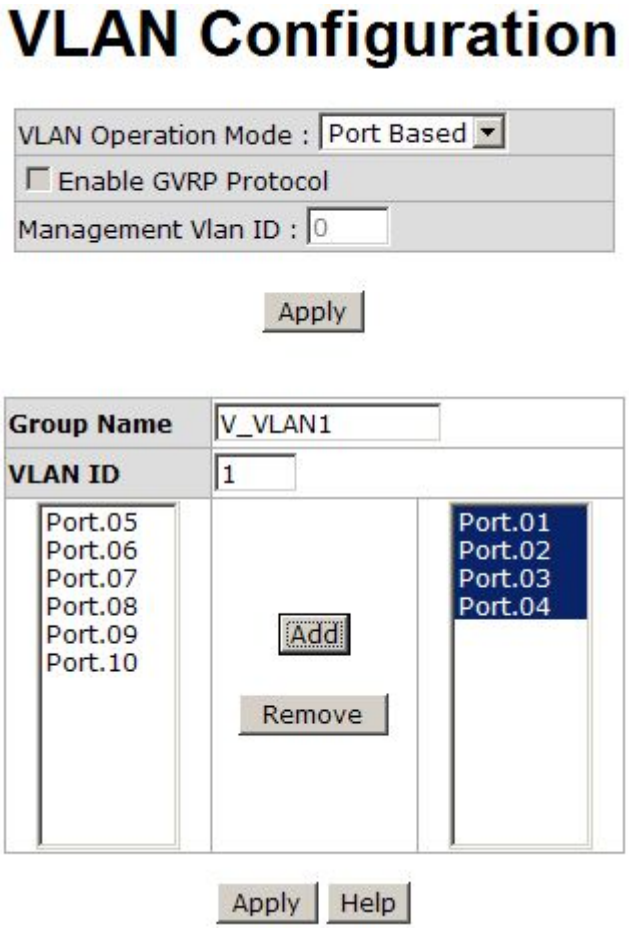


VLAN – Port Based interface

- Pull down the selection item and focus on **Port Based** then press Apply button

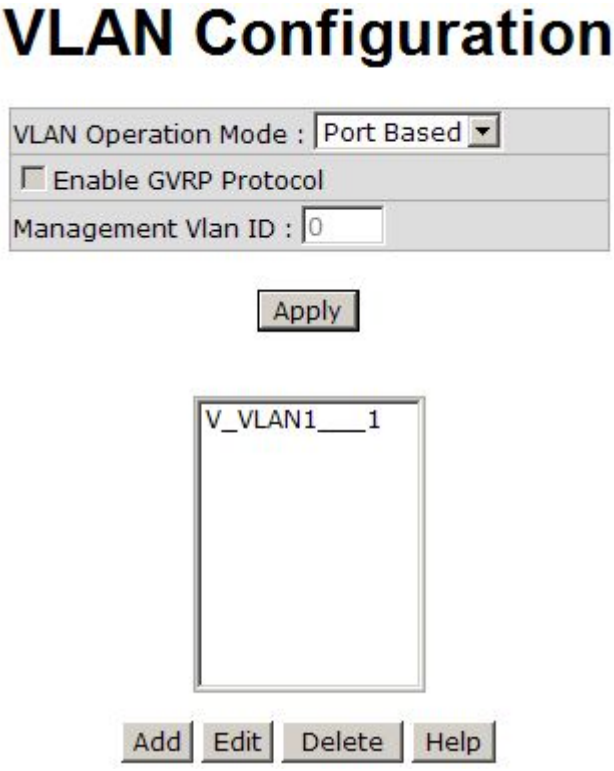
to set the VLAN Operation Mode in **Port Based** mode.

- Click Add button to add a new VLAN group (The maximum VLAN group is up to 64 VLAN groups).



VLAN—Port Based Add interface

- Enter the group name and VLAN ID. Add the port number having selected into the right field to group these members to be a VLAN group or remove any of them listed in the right field from the VLAN.
- And then, click Apply button to have the settings taken effect.
- You will see the VLAN displays.



VLAN—Port Based Edit/Delete interface

- Use Delete button to delete the VLAN.
- Use Edit button to modify group name, VLAN ID, or add/remove the members of the existing VLAN group.

[NOTE] Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch power off.

802.1Q VLAN

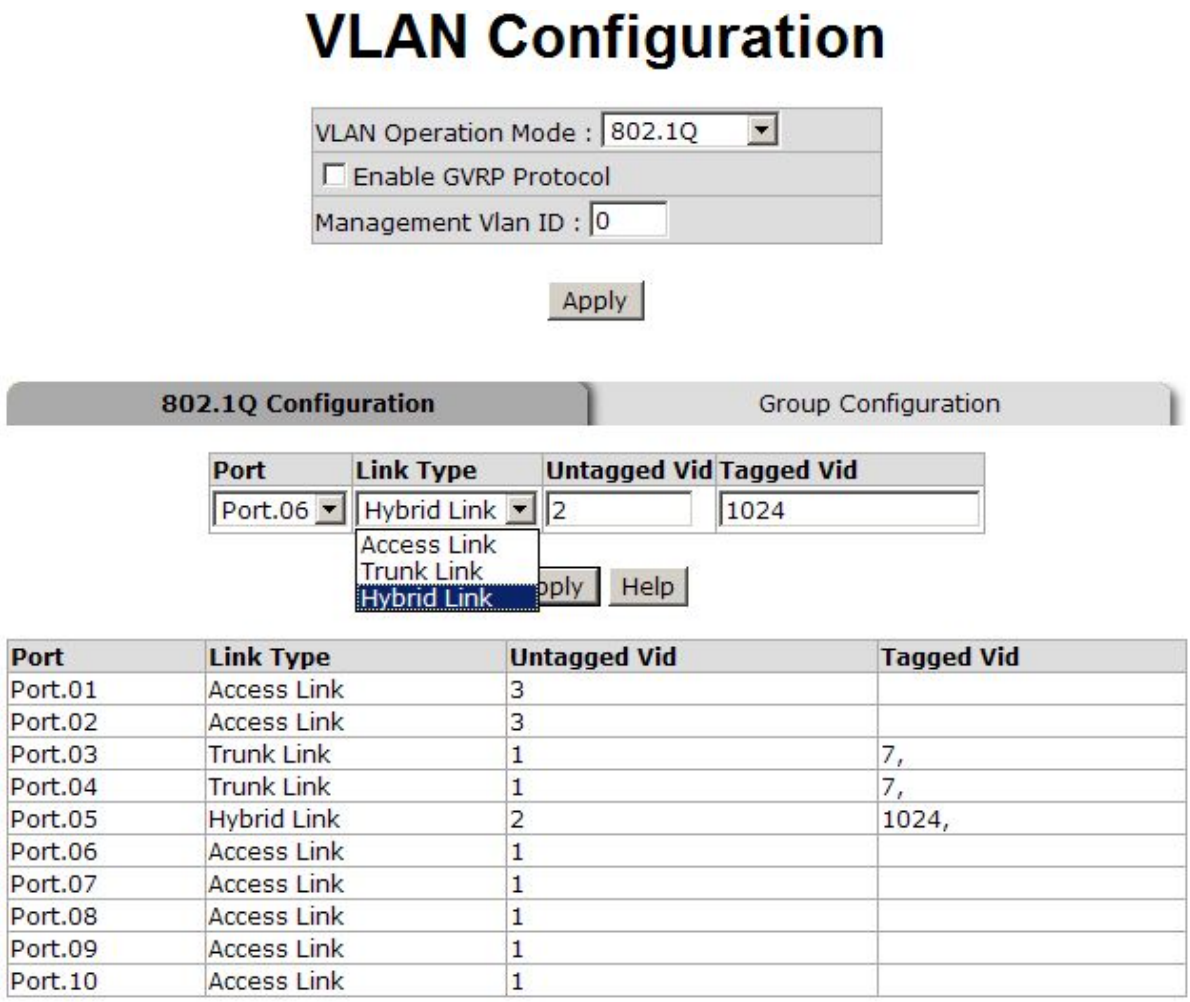
Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.
You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configuration. Enable 802.1Q VLAN, all ports on the switch belong to default VLAN of VID 1. The default VLAN can’t be deleted.

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.
GVRP is based on GARP (Generic Attribute Registration Protocol), a protocol that defines procedures by which end stations and switches in a local area network (LAN) can register and de-register attributes, such as identifiers or addresses, with each other.
Every end station and switch thus has a current record of all the other end stations and switches that can be reached.

802.1Q Configuration

- Pull down the selection item and focus on **802.1Q** then press Apply button to set the VLAN Operation Mode in **802.1Q** mode.

- **Enable GVRP Protocol:** Tick the checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is in **802.1Q** mode.
- Select the port you want to configure.
- **Link Type**: There are 3 types of link type.
  - **Access Link:** Single switch only, it allows the user to group ports by assigning the same Untagged VID. While this link type is set, the Untagged VID column field is available but the Tagged VID column field is disabled.
  - **Trunk Link:** The extended application of **Access Link**. It allows the user to group ports by assigning the same Tagged VID across 2 or more switches. Having set this link type, the Tagged VID column field is available but the Untagged VID column field is disabled.
  - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
- **Untagged VID:** Assign the untagged frame VID.
- **Tagged VID:** Assign the tagged frame VID.
- Click Apply button to have the settings taken effect.
- You can see the link type, untagged VID, and tagged VID information of each port in the table below on the screen.



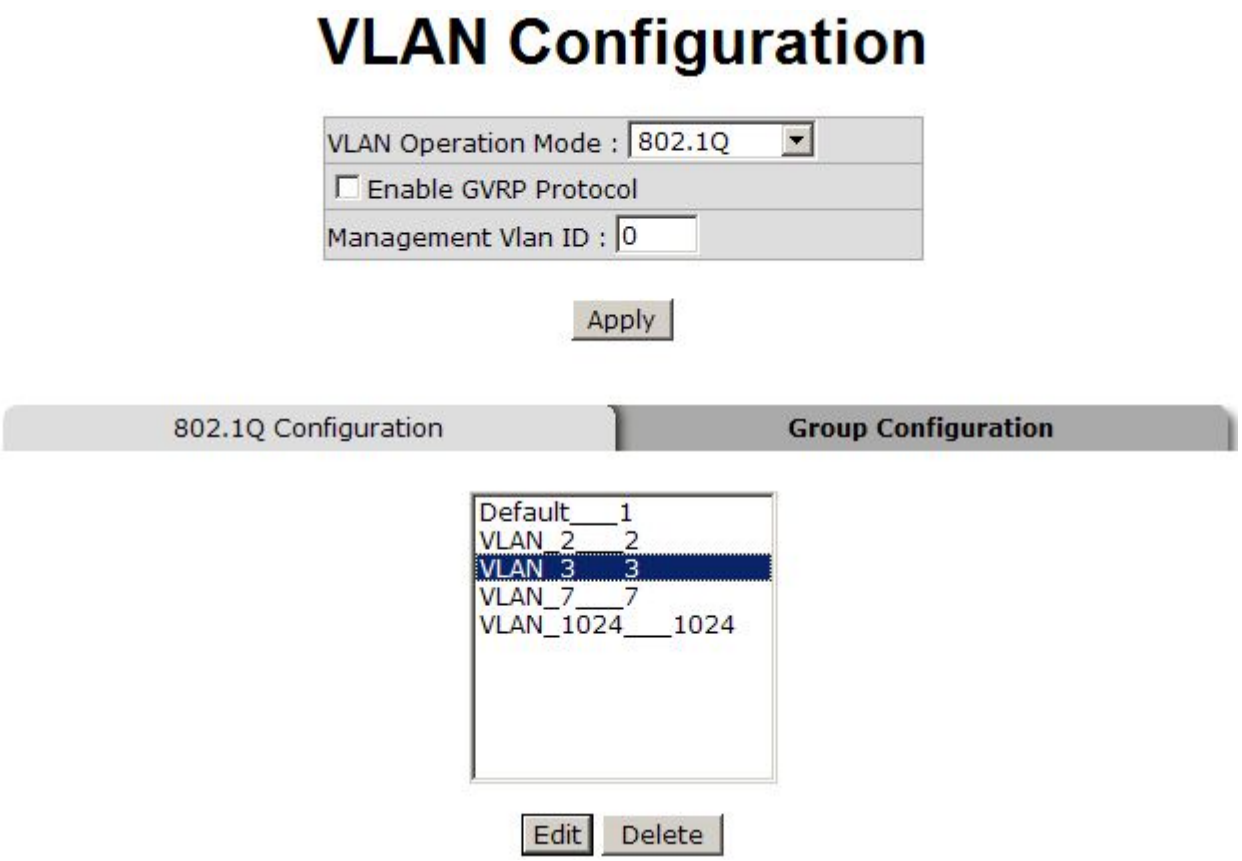
Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	3	
Port.02	Access Link	3	
Port.03	Trunk Link	1	7,
Port.04	Trunk Link	1	7,
Port.05	Hybrid Link	2	1024,
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
Port.09	Access Link	1	
Port.10	Access Link	1	

802.1Q VLAN interface

Group Configuration

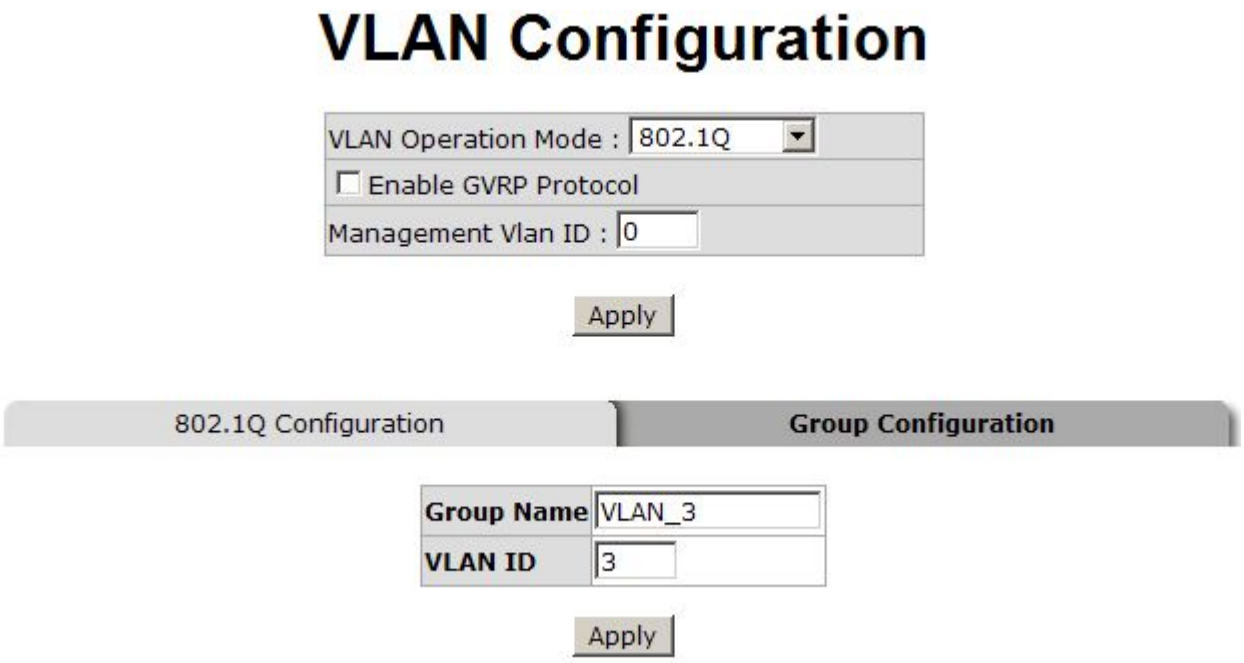
Edit the existing VLAN Group.

- Select the VLAN group in the table list.
- Click Edit button.



Group Configuration interface

- You can modify the VLAN group name and VLAN ID.



Group Configuration interface

- Click Apply button.

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto-detect the connected device that is running STP or RSTP protocol.

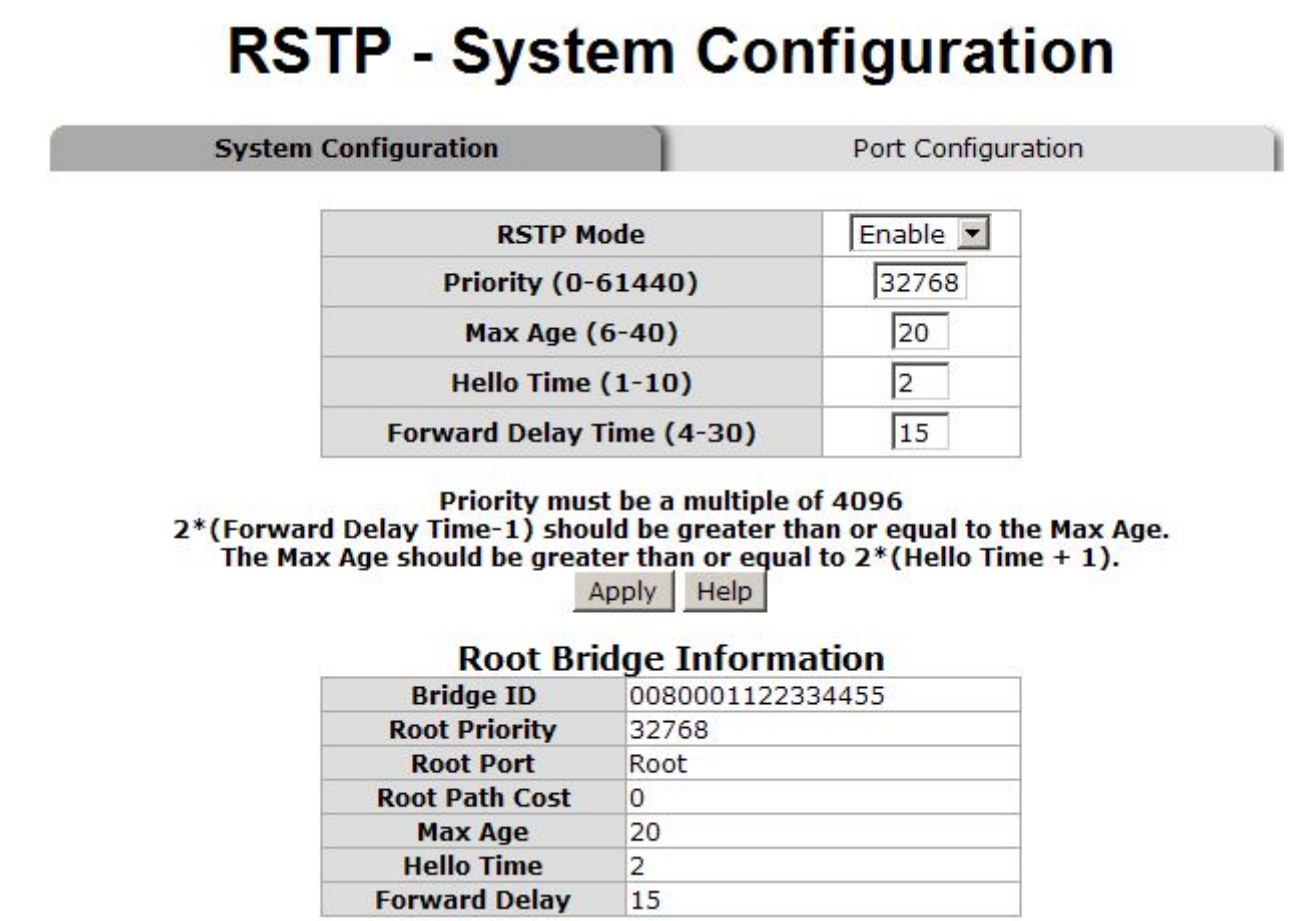
RSTP - System Configuration

- The user can view spanning tree information of Root Bridge.
- The user can modify RSTP state. After modification, click Apply button.
  - **RSTP mode:** The user must enable the RSTP function first before configuring

the related parameters.

- **Priority (0-61440):** The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
- **Max Age (6-40):** The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
- **Hello Time (1-10):** The time that controls the switch to send out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
- **Forward Delay Time (4-30):** The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

[NOTE]	Follow the rule as below to configure the MAX Age, Hello Time, and Forward Delay Time. **2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)**



RSTP System Configuration interface

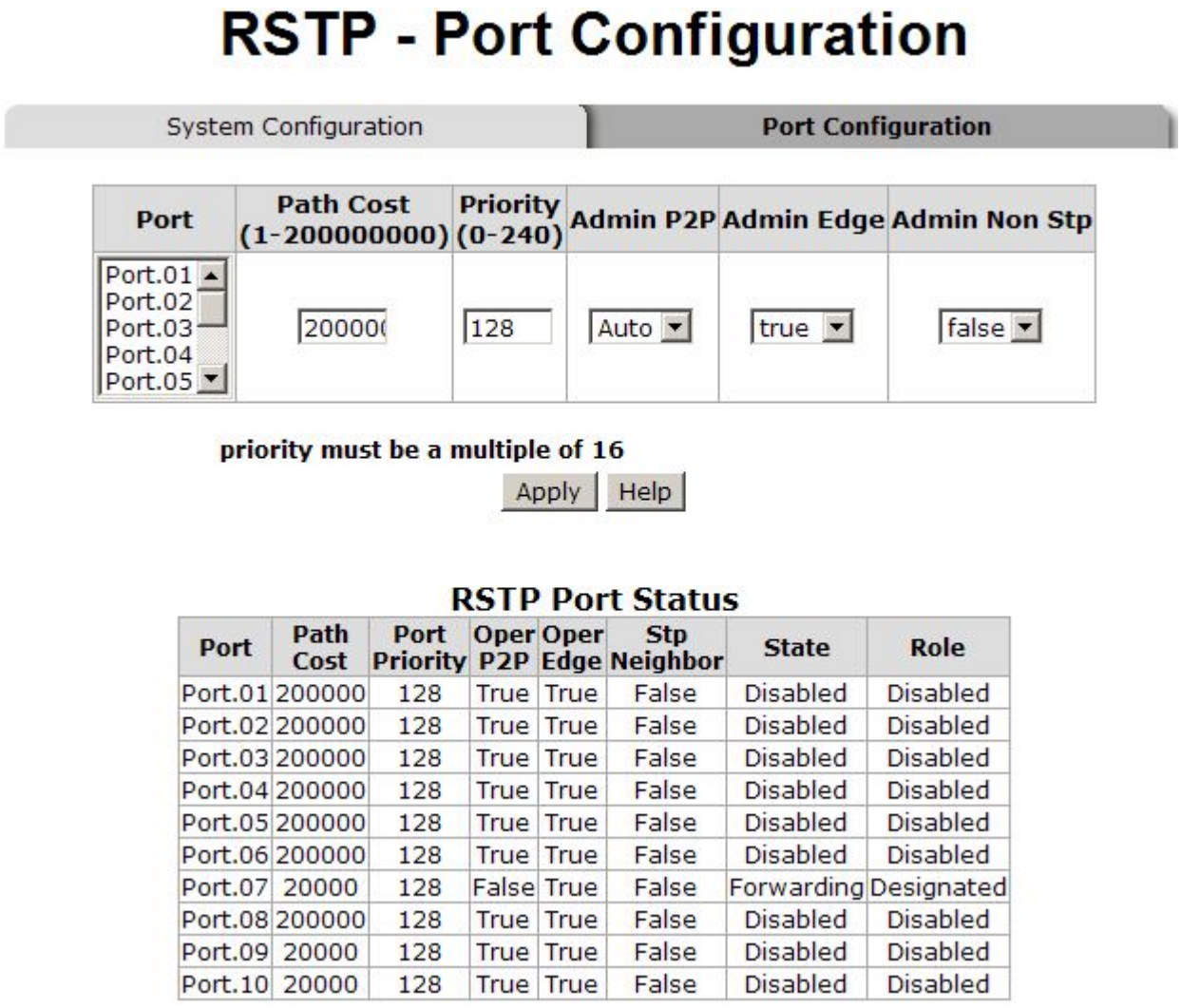
RSTP - Port Configuration

You can configure path cost and priority of every port.

- Select the port in the port column field.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240 (the port of the highest value will be blocked). The value of priority must be the multiple of 16.
- **Admin P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This

function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.

- **Admin Edge:** The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
- **Admin Non Stp:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
- Click Apply.



RSTP Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

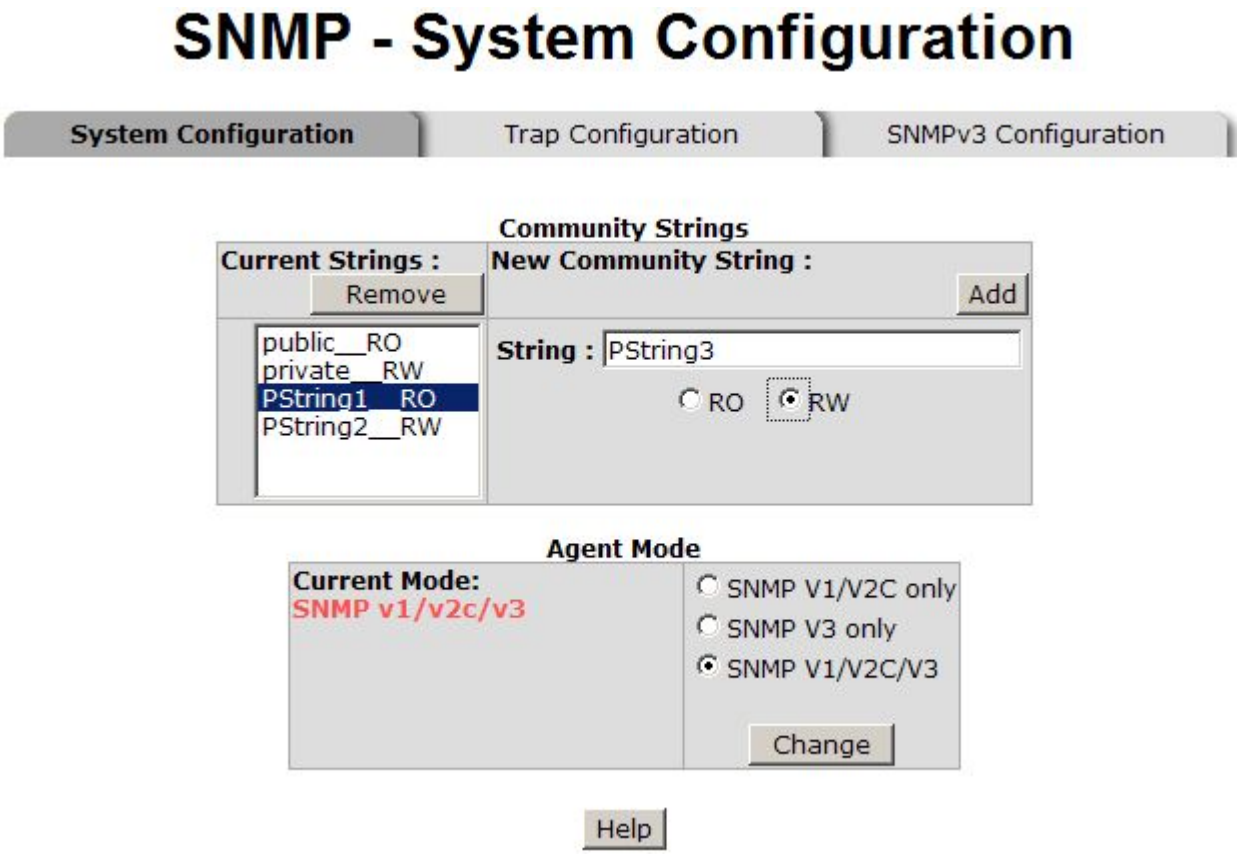
- **Community Strings**

Here you can define the new community string set and remove the unwanted community string.

- **String:** Fill the name string.
- **RO:** Read only. Enables requests accompanied by this community string to display MIB-object information.
- **RW:** Read write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
- Click Add button.
- To remove the community string, select the community string that you have defined and click Remove button. You cannot edit the name of the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use and then click Change

button to switch to the selected SNMP version mode. The default value is ‘SNMP v1/v2c only’



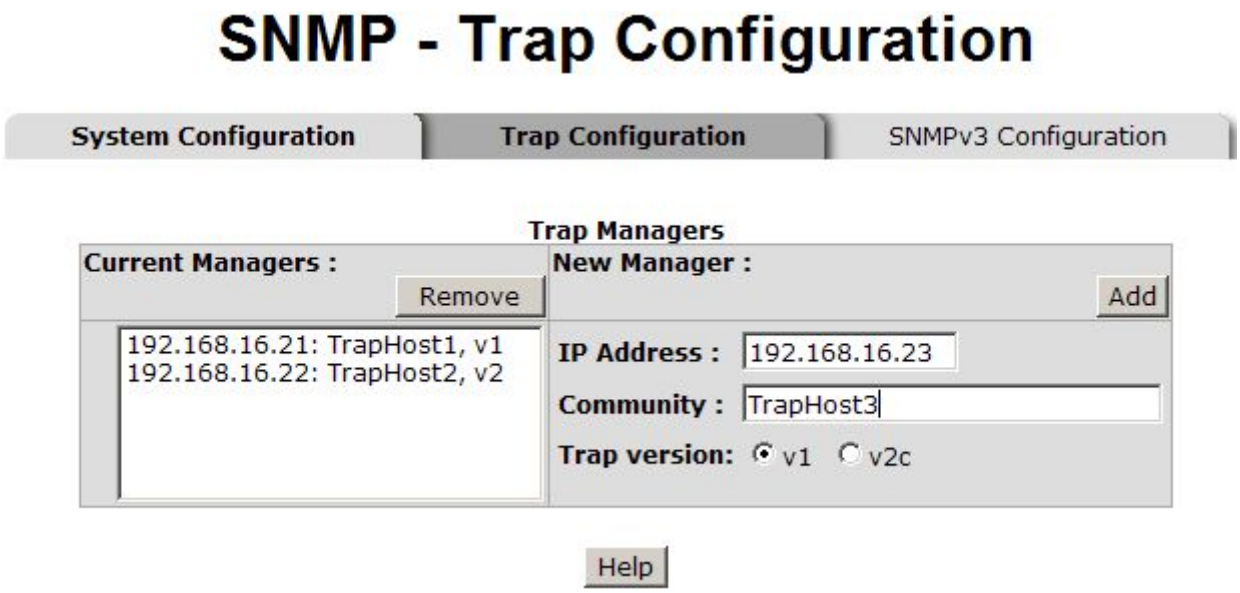
SNMP System Configuration interface

Trap Configuration

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP address of the station and a community string. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

- **IP Address:** Enter the IP address of the trap manager.
- **Community:** Enter the community string.

- **Trap Version:** Select the SNMP trap version type—v1 or v2c.
- Click Add button.
- To remove the community string, select the community string listed in the current managers field and click Remove button.



Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

Context Table

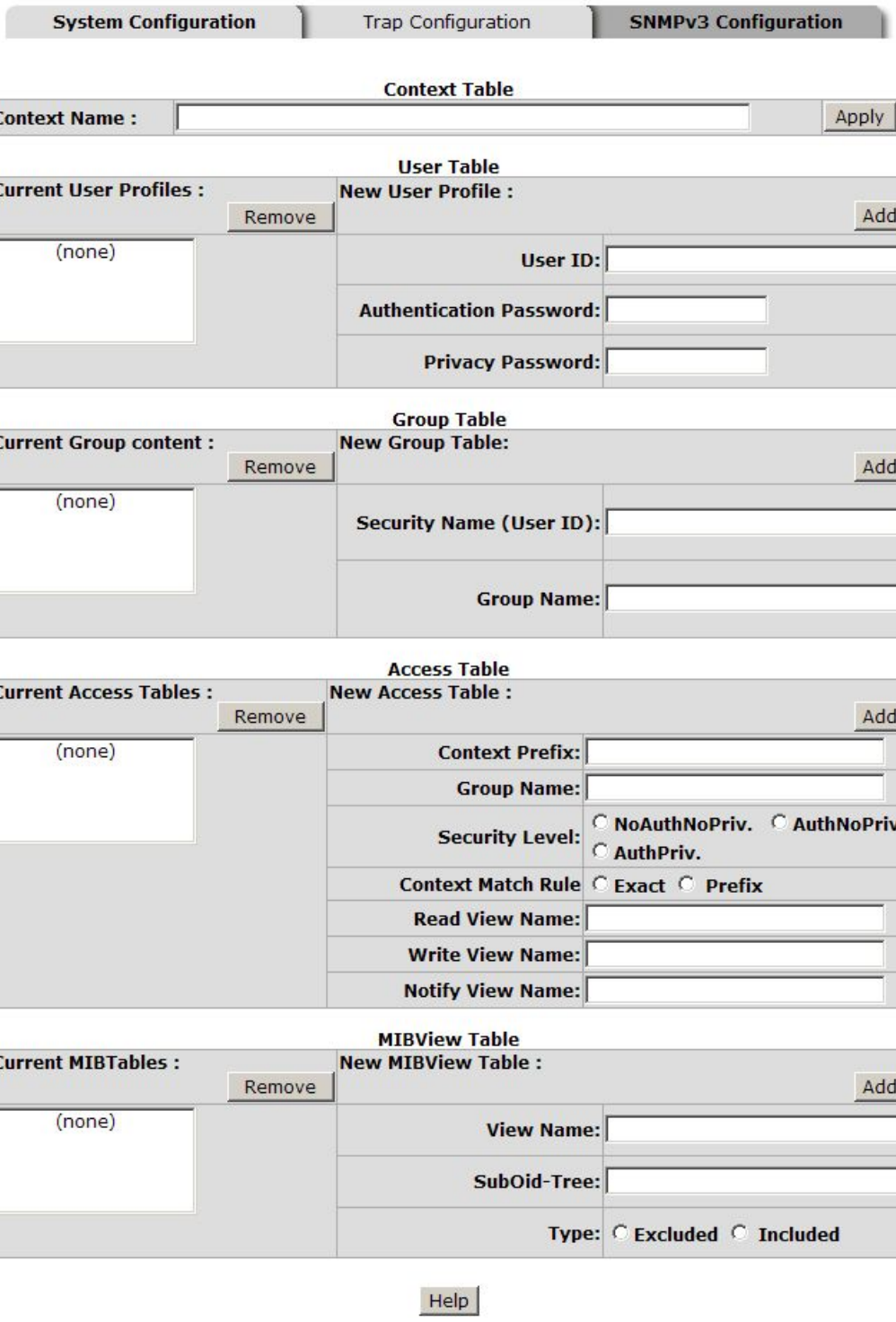
Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name. Click Remove to remove the unwanted context name.

User Profile

Configure SNMP v3 user table..

- **User ID:** Set up the user name.
- **Authentication Password:** Set up the authentication password.
- **Privacy Password:** Set up the private password.
- Click Add to add the context name.
- Click Remove to remove the unwanted context name.

SNMP - SNMPv3 Configuration



Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in user table.
- **Group Name:** Set up the group name.
- Click Add to add the context name.
- Click Remove to remove the unwanted context name.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Click Add to add the context name.
- Click Remove to remove the unwanted context name.

MIBview Table

Configure MIB view table.

- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type—excluded or included.
- Click Add to add the context name.
- Click Remove to remove the unwanted context name.

QoS Configuration

Here you can configure Qos policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **Qos Policy:** Select the QoS policy rule.
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, while the system processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Use a strict priority scheme:** Always the higher queue will be processed first, except the higher queue is empty.
  - **Priority Type:** There are 5 priority type selections available—**Port-based**, **TOS only**, **COS only**, **TOS first**, and **COS first**. Disable means no priority type is selected.
- Click Apply button to make the settings effective.

QoS Configuration

Qos Policy:

Use an 8,4,2,1 weighted fair queuing scheme
Use a strict priority scheme
Priority Type: Disable

Apply Help

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08	Port.09	Port.10
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

COS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

TOS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	8	9	10	11	12	13	14	15
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	16	17	18	19	20	21	22	23
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	24	25	26	27	28	29	30	31
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	32	33	34	35	36	37	38	39
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	40	41	42	43	44	45	46	47
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	48	49	50	51	52	53	54	55
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	56	57	58	59	60	61	62	63
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

QoS Configuration interface

Port-based Priority

Configure the priority level for each port. With the drop-down selection item of **Priority Type** above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

- **Port x:** Each port has 4 priority levels—High, Middle, Low, and Lowest—to be chosen.
- Click Apply button to make the settings effective.

COS Configuration

Set up the COS priority level. With the drop-down selection item of **Priority Type** above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.

- **COS priority:** Set up the COS priority level 0~7—High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority. With the drop-down selection item of **Priority Type** above being selected as TOS only/TOS first, this control item will then be available to set the queuing policy for each port.

- **TOS priority:** The system provides 0~63 TOS priority level. Each level has 4 types of priority—High, Middle, Low, and Lowest. The default value is 'Lowest' priority for each level. When the IP packet is received, the system will check the TOS level value in

the IP packet that has received. For example, the user sets the TOS level 25 as high, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25 (priority = high), and then the packet priority will have highest priority.

- Click Apply button to make the settings effective.

IGMP Configuration

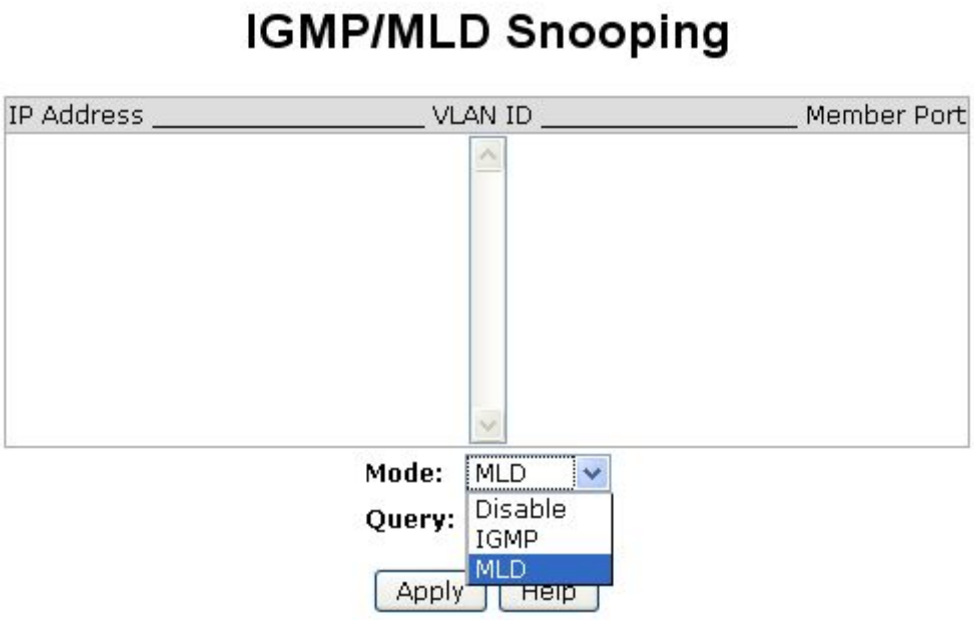
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch. IGMP have three fundamental types of message shown as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then the IGMP snooping information displays. IP

multicast addresses range are from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.
- **MLD Query:** enable or disable the MLD query function. The MLD query information will be displayed in MLD status section.
- Click Apply button.



IGMP Configuration interface

Pro-Ring II System

Pro-Ring II is a new Ring mechanism for Equitel Industrial Switches in which it eliminates the need to pre-set the Master switch in old Pro-Ring and yet to protect the network by much secure topologies than ever. Pro-Ring II works as a Ring Chain to reduce the risk of master switch linking down whereas the setup becomes much easier. Pro-Ring II can be backward compatible with old Pro-Ring by down-grading the Ring

scheme to old one.

Legacy-Ring

- **Enable Legacy-Ring:** To enable the X-Ring function, tick the checkbox beside the **X-Ring2 Operation Mode** string label. If this checkbox is not ticked, all the ring functions are unavailable.
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign the ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.
- And then, click Apply button to apply the configuration.

X-Ring2

- **Enable X-Ring2:** To enable the X-Ring2 function, tick the checkbox beside the **X-Ring2 Operation Mode** string label. If this checkbox is not ticked, the ring functions are unavailable.
  - **Ring ID:** Set the Ring ID value to carry different RID frames to other switch.
  - **1st & 2nd Ring Ports:** Pull down the selection menu to assign the ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the

backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.

- **Mode:** Normal, Active, passive.
- **1st & 2nd Redundant Ports:** Pull down the selection menu to assign the ports as the member ports. **1st Rnd Port** is the working port and **2nd Rnd Port** is the backup port. When **1st Rnd Port** fails, the system will automatically upgrade the **2nd Rnd Port** to be the working port.
- **1st & 2nd Redundant Ports ID:** Set the Rnd ID port value to carry different Rnd ID frames to other switch.

■ And then, click Add to have the configuration take effect.

X-Ring2
X-Ring2 Operation Mode : X-Ring2
X-Ring2 Configuration
Index_Ring ID_1st Ring Port_2nd Ring Port_Mode_1st Rdn Port_1st Rdn Port ID_2nd Rdn Port_2nd Rdn Port ID
1_____1___Port.01_____Port.02_____NORM_Port.09_1_Port.10_1
Ring ID 1st Ring Port 2nd Ring Port Mode 1st Rdn Port 1st Rdn Port ID 2nd Rdn Port 2nd Rdn Port ID
NONE NONE NORM NONE NONE
Add Delete
X-Ring2 Ring Information
X-Ring2 Version 0.043.49
Index Ring ID 1st Ring Port 2nd Ring Port Mode 1st Rdn Port 1st Rdn Port ID 2nd Rdn Port 2nd Rdn Port ID
1 1 Port.01_BLK Port.02_FWD NORM Port.09_FWD 1 Port.10_BLK 1

[NOTE]

1. When the X-Ring2 function enabled, the user must disable the RSTP. The X-Ring2 function and RSTP function cannot exist on a switch at the same time.
2. Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when switch powers off.

Security

In this section, you can configure the 802.1x and MAC address table.

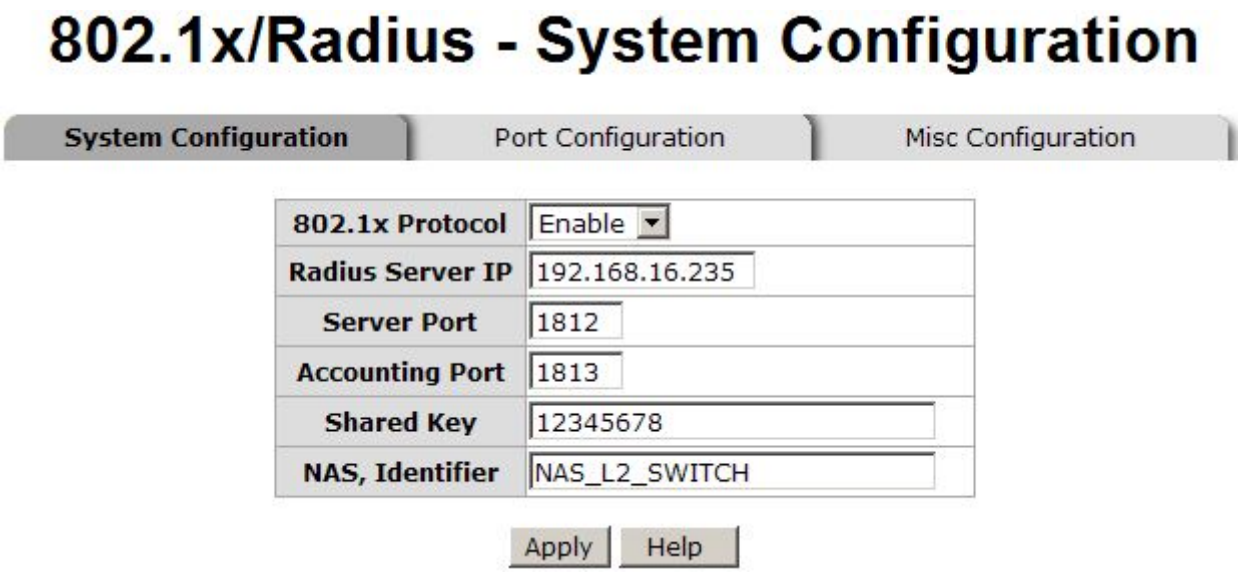
802.1X/Radius Configuration

802.1x is an IEEE authentication specification which prevents the client from connecting to a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

- **IEEE 802.1x Protocol:** Enable or disable 802.1x protocol.
- **Radius Server IP:** Assign the RADIUS Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified RADIUS Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified RADIUS Server.
- **Shared Key:** Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
- **NAS, Identifier:** Set the identifier for the RADIUS client.
- Click Apply button.

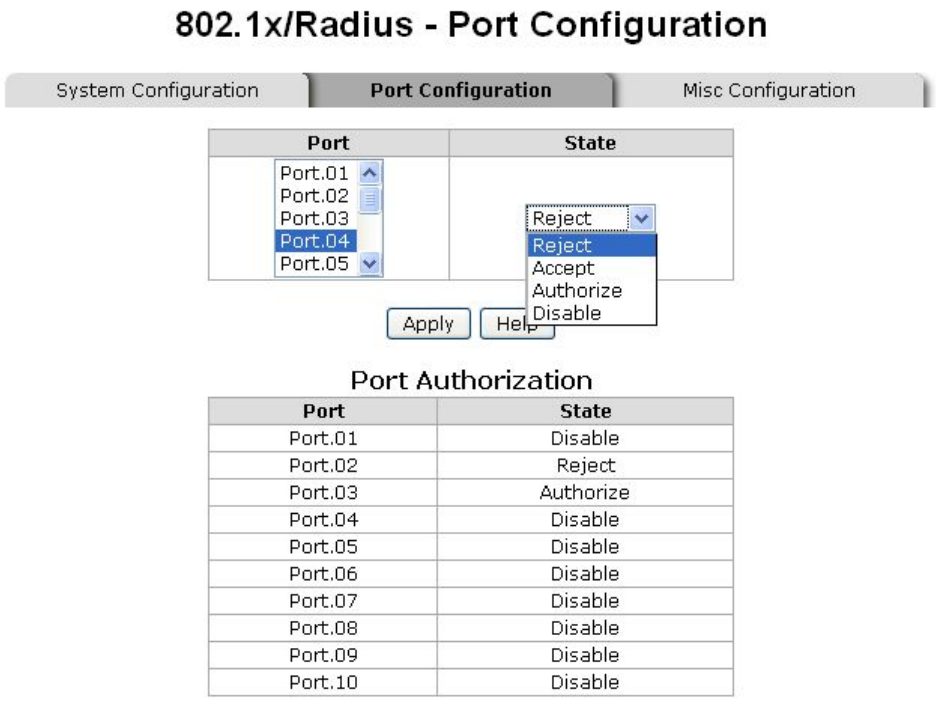


802.1x System Configuration interface

802.1x Per Port Configuration

You can configure the 802.1x authentication state for each port. The state provides Disable, Accept, Reject, and Authorize.

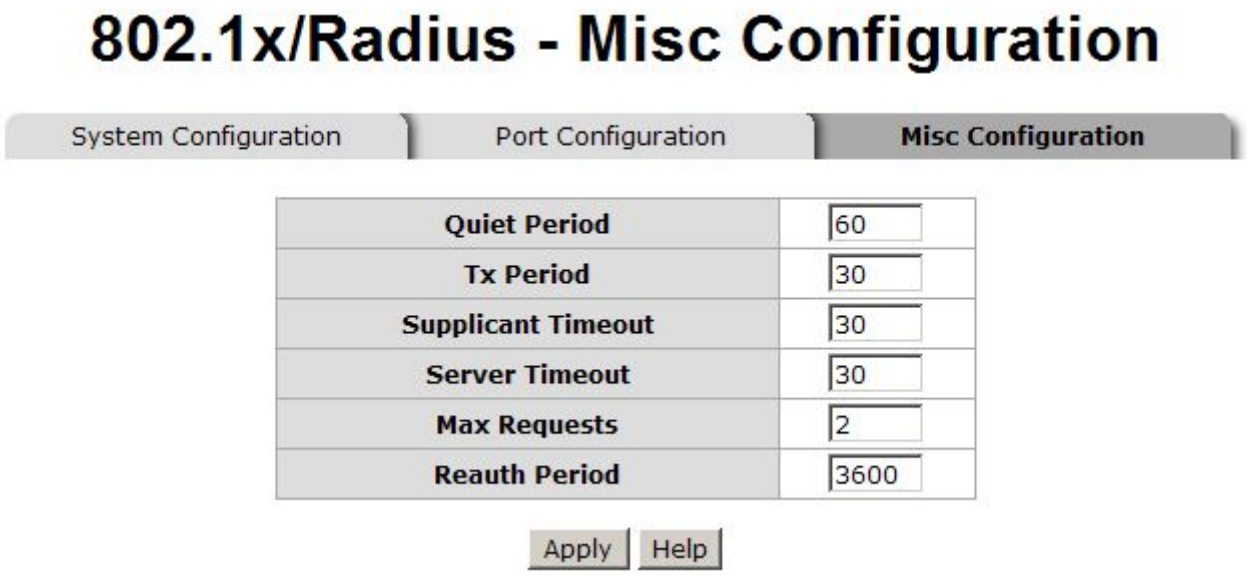
- **Reject:** The specified port is required to be held in the unauthorized state.
- **Accept:** The specified port is required to be held in the Authorized state.
- **Authorized:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** When disabled, the specified port works without complying with 802.1x protocol.
- Click Apply button.



802.1x Per Port Setting interface

Misc Configuration

- **Quiet Period:** Set the period which the port doesn't try to acquire a supplicant.
- **TX Period:** Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** Set the period of time which clients connected must be re-authenticated.
- Click Apply button.



802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure the port security.

Static MAC Address

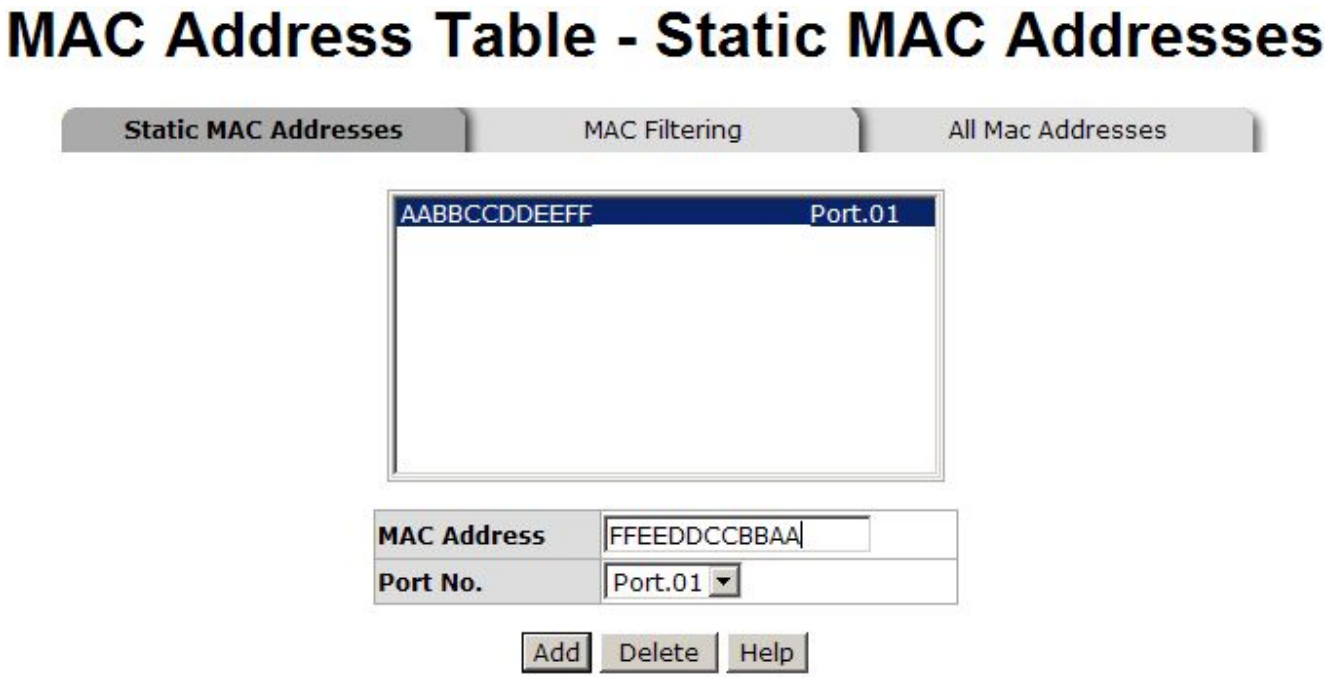
You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

Add the Static MAC Address

You can add static MAC address in the switch MAC table here.

- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.

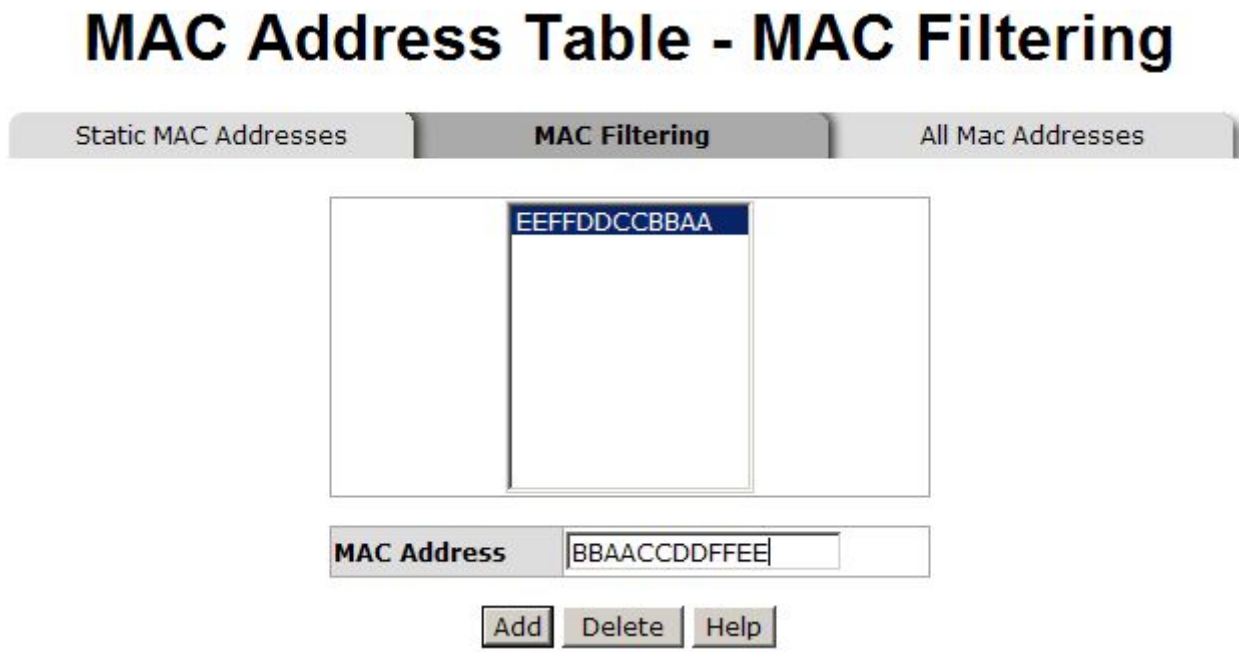
- **Port No.:** Pull down the selection menu to select the port number.
- Click Add button.
- If you want to delete the MAC address from filtering table, select the MAC address and click Delete button.



Static MAC Addresses interface

MAC Filtering

By filtering MAC address, the switch can easily filter the pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.



MAC Filtering interface

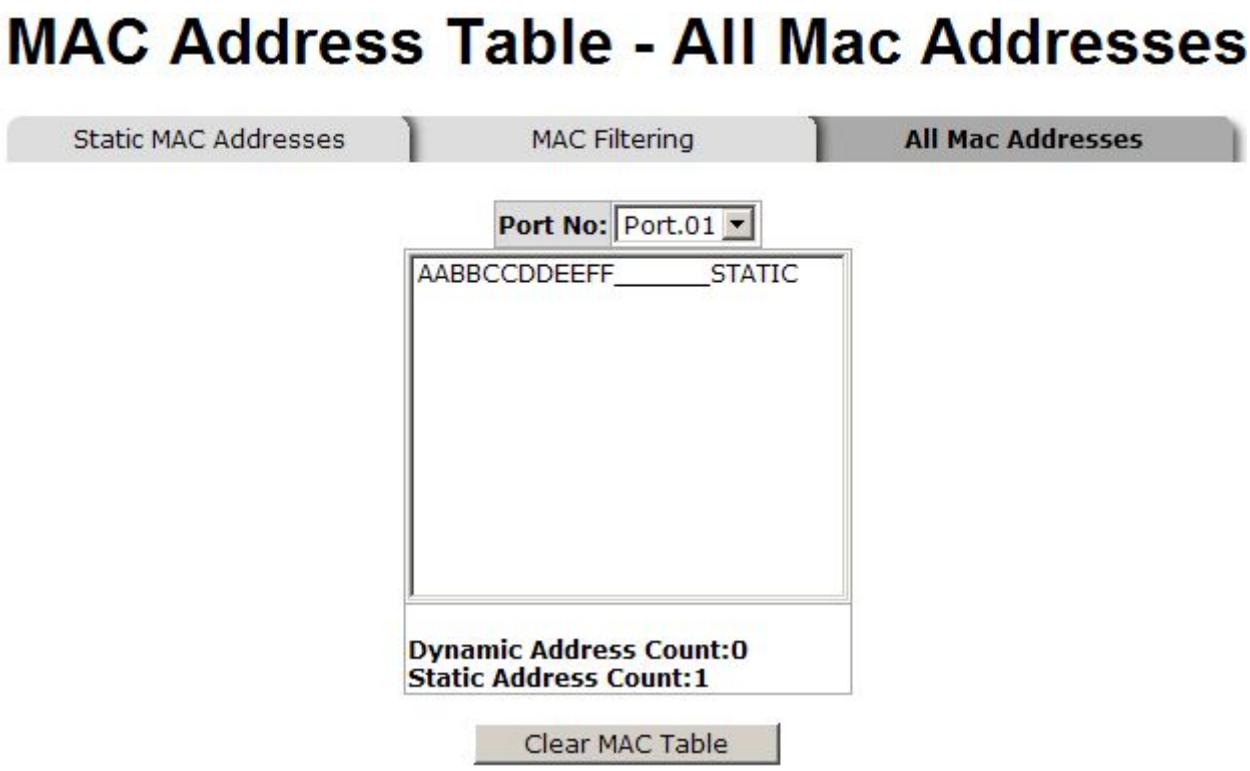
1. **MAC Address:** Enter the MAC address that you want to filter.
2. Click Add button.
3. If you want to delete the MAC address from the filtering table, select the MAC address and click Delete button.

All MAC Addresses

You can view the port that connected device's MAC address and the related devices' MAC address.

1. Select the port.
2. The selected port of static & dynamic MAC address information will be displayed in here.
3. Click Clear MAC Table to clear the current port static MAC address information on

screen.



All MAC Address interface

Factory Default

Reset switch to default configuration. Click Reset button to reset all configurations to the default value.

Factory Default interface

Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration will be saved. Click Save to save the all configuration to the flash memory.

Save Configuration interface

System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.

System Reboot interface

Troubles shooting

- Verify that you are using the right power cord/adapter (DC 9 ~ 56V). Please don't use the power adapter with DC output higher than 56V, or this switch will be burned down.
- Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps connections, or 100 Ω Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- **Diagnosing LED Indicators:** To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.
- If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact the local dealer for assistance.
- If the LED indicators are normal and the connected cables are correct but the packets still cannot be transmitted. Please check the user system's Ethernet devices' configuration or status.

Technical Specification

The 7 10/100TX + 3 10/100/1000T with 100/1000M SFP Combo Industrial Managed Switch with DIDO technical specification are as follows.

Standard	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3ab 1000Base-T IEEE 802.3z Gigabit fiber IEEE 802.3x Flow Control and Back-pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1d Spanning Tree IEEE 802.1w Rapid Spanning Tree IEEE 802.1p Class of Service IEEE 802.1Q VLAN Tag IEEE 802.1x User Authentication (RADIUS) IEEE 802.1ab LLDP
Protocol	CSMA/CD
Transfer Rate	14,880 pps for 10Base-T Ethernet port 148,800 pps for 100Base-TX/FX Fast Ethernet port 1,488,000 pps for Gigabit Fiber Ethernet port
MAC address	8K MAC address table
Packet Buffer	1Mbits
Flash ROM	4Mbytes
DRAM	32Mbytes
Connector	10/100TX: 7 x RJ-45 10/100/1000T/ Mini-GBIC Combo: 3 x RJ-45 + 3 x

	100/1000 SFP sockets RS-232 connector: RJ-45 type
DI/DO	2 Digital Input (DI) : Level 0 : -30~2V Level 1 : 10~30V Max. input current: 8mA 2 Digital Output (DO): Open collector to 24 VDC, 1A
LED	**Per unit:** Power (Green), Power 1 (Green), Power 2 (Green), Fault (Red), Master (Green) **10/100TX:** Link/Activity (Green), Full duplex/Collision (Yellow) **Gigabit Copper:** Link/Activity (Green), Speed (1000Mbps Green) **SFP:** Link/Activity (Green)
Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5 cable EIA/TIA-568 100-ohm (100m) 1000Base-T: 2-pair UTP/STP Cat. 5e or 6 cable EIA/TIA-568 100-ohm (100m)
Optical cable	■ **LC (Multi-mode):** 50/125um or 62.5/125um ■ **LC (Single mode):** 9/125um
Back-plane	7.4Gbps
Packet throughput ability	11Mpps at 64bytes

Power Supply	9 ~ 56V_{DC} / 12 ~ 36V_{AC} (Optional) Redundant power with polarity reverse protection and removable terminal block (The power supply should meet the “document listed by UL” and its output must comply with L.P.S)
Power Consumption	10.2 Watts
Install	DIN Rail and Wall Mount Design
Operating Temperature	-20^{o}C to 60^{o}C (Standard model) -40^{o}C to 75^{o}C (-E model)
Operation Humidity	5% to 95% (Non-condensing)
Storage Temperature	-40^{o}C to 85^{o}C
Case Dimension	IP-30, 217mm(W) x 141mm(D) x 66mm(H)
EMI	FCC Class A CE EN61000-4-2 (ESD) CE EN61000-4-3 (RS) CE EN61000-4-4 (EFT) CE EN61000-4-5 (Surge) CE EN61000-4-6 (CS) CE EN61000-4-8 CE EN61000-4-11 CE EN61000-4-12 CE EN61000-6-2 CE EN61000-6-4

Safety	UL cUL CE/EN60950-1
Stability testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)